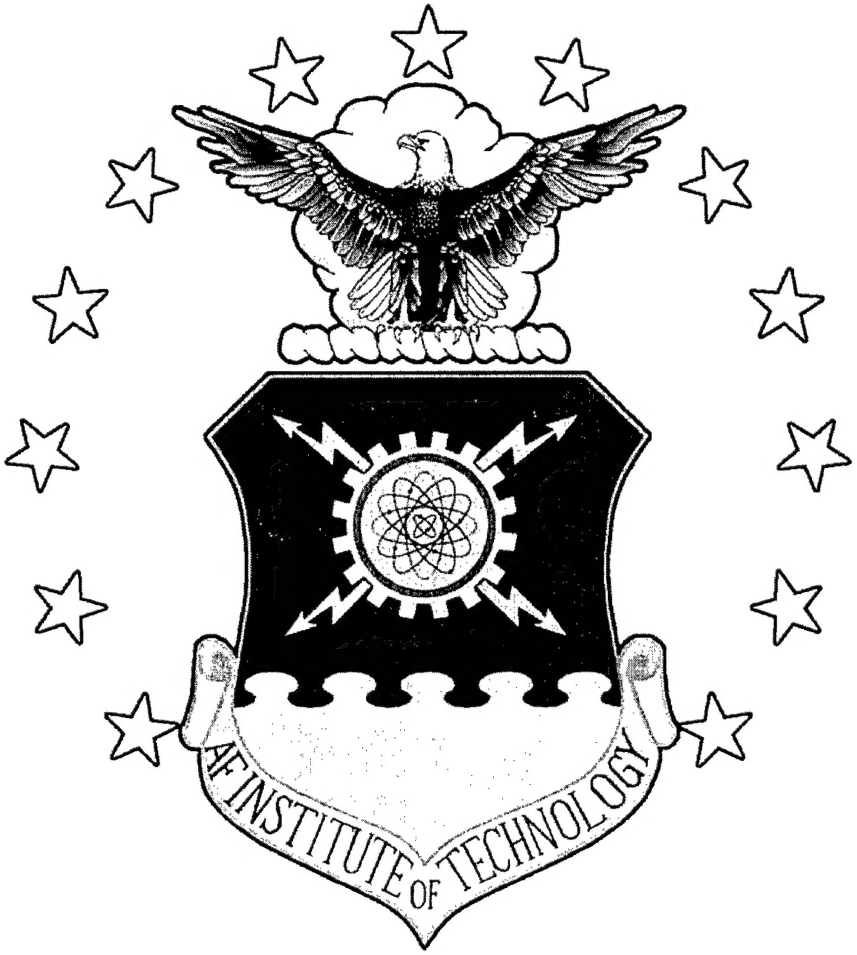


THE EFFECT OF CONTEXTUAL-BASED TRAINING ON ARTIFACT-BASED DECEPTION DETECTION

THESIS

Elizabeth A. Autrey, Captain, USAF
AFIT/GIR/ENV/01M-15

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

20010612 119

Approved for Public Release; Distribution Unlimited

AFIT/GIR/ENV/01M-15

THE EFFECT OF CONTEXTUAL-BASED TRAINING ON ARTIFACT-BASED DECEPTION DETECTION

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

Elizabeth A. Autrey, B.S.

Captain, USAF

March 2001

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

AFIT/GIR/ENV/01M-15

THE EFFECT OF CONTEXTUAL-BASED TRAINING ON ARTIFACT-BASED DECEPTION DETECTION

Elizabeth A. Autrey, B.S.
Captain, USAF

Approved:

David P. Biros (Chairman)	date
Alan R. Hevner (Member)	date
Gregg H. Gunsch (Member)	date

Acknowledgements

I wish to express sincere thanks to my advisor, Major David Biros, for providing guidance when it was needed. His prior work in the primary subject matter helped to keep me on track within the scope of the research. Thanks also go to my committee members, Dr Alan Heminger and Dr Gregg Gunsch, for their constructive thoughts and inputs to this thesis effort. Finally, I would like to thank Capt Greg Fields and Capt Brent Langhals for their help and knowledge with the experiment, as well as Capt Jon Autrey for his assistance in using the statistical tools needed for this study.

Elizabeth A. Autrey

Table of Contents

Page

Page

List of Figures

List of Tables

Abstract

Air Force dependence on information technology (IT) creates vulnerabilities that it cannot ignore. With global availability of commercial IT and the Internet, the Air Force does not necessarily have the high technological advantage over potential adversaries that it once had. Furthermore, it is possible to directly and covertly manipulate information within information systems, or artifacts, without notice. This directly affects decision makers since the availability and integrity of information is critical. Air Force physical and network security measures taken to protect its information do not guarantee detection of direct information manipulation. This leaves it to information artifact users to detect such deception.

This thesis explores whether information artifact users can be trained in artifact-based deception detection. Research in this area is lacking. This study attempted to apply the contextual-based principles of Information Manipulation Theory (IMT), a theory from interpersonal deception, to human-artifact deception. An experiment comparing differences in subject performance between two Command and Control computer simulations was conducted. A training program developed from IMT principles was applied between simulations. Results of the experiment were inconclusive. Lessons learned for future research suggest training programs in human-artifact deception detection need to be both information system- and domain-specific.

THE EFFECT OF CONTEXTUAL-BASED TRAINING ON ARTIFACT-BASED DECEPTION DETECTION

I. Background and Statement of the Problem

Introduction

Military doctrine recognizes that the information explosion caused by current information technology (IT) has substantially changed the way the military conducts its operations: "Information, information processing, and communications networks are at the core of every military activity" (JV-2020, 2000:8). Air Force Doctrine Document 2-5 expresses the difficulty in identifying any Air Force system that does not rely on sophisticated electronics and information. The Air Force's dependence on IT is profound, and it will only increase (AFDD 2-5, 1998). With technology advancing at its current phenomenal pace, this dependence causes new vulnerabilities not only for the Air Force, but the joint forces as well (JV-2020, 2000). Furthermore,

> ...[P]otential adversaries will have access to the global commercial industrial base and much of the same technology as the US military. We will not necessarily sustain a wide technological advantage over our adversaries in all areas. Increased availability of commercial satellites, digital communications, and the public internet all give adversaries new capabilities at a relatively low cost (JV-2020, 2000:4).

It is also wisely pointed out that,

> As technology advances, society's ability to transfer information and an adversary's opportunity to affect that information increases and, in some cases, may eclipse the security designed into the information systems. Just as the United States plans to employ IO against its adversaries, so too can it expect adversaries to reciprocate (AFDD 2-5, 1998:5-6).

Background

The focus on information and IT might suggest that the search for and efforts to exploit information are fairly new. However, "the competition for information is as old as human conflict" (Fogleman, 1995:1-11). The competition for information has not changed, but rather the "means and route of attack" for obtaining it (AFDD 2-5, 1998:ii). Joint Vision 2020 regards Information Superiority as a key enabler of full spectrum dominance and victory. The Air Force has named Information Superiority as one of its core competencies "upon which all the other core competencies rely" (AFDD 2-5, 1998:2). Information Superiority is defined as, "The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same" (JV-2020, 2000:8).

Information is critical in all military aspects. Commanders cannot plan operations, deploy forces, or execute missions without it: "The commander with better information holds a powerful advantage over his adversary" (Fogleman, 1995:1-11). It follows that the information needed to make such decisions must be the right information. This, along with vulnerabilities associated with dependence on IT, renders Information Assurance (IA) a necessity (AFDD 2-5, 1998). IA is defined as "...those measures to

protect and defend information and information systems by ensuring their availability, integrity, authenticity, confidentiality, and nonrepudiation (ability to confirm source of transmission and data)" (Ibid:17). As such, information systems must be protected from unauthorized access and information corruption.

"Cornerstones of Information Warfare" gives a simple but bottom-line description of information use: "Militaries have always tried to gain or affect the information required for an adversary to effectively employ forces" (Fogleman, 1995:1-11). This is still true today. As "Cornerstones" also points out, historically, enemy information was attacked indirectly by using deception to influence the adversary's decisions. The goal of such deception would be to cause the adversary to observe the deception, perceive it as reality, and then use it to make decisions, hopefully in the deceiver's favor (Fogleman, 1995).

The advent of information systems and computer networks has changed how information can be used. Technology today allows an adversary to directly manipulate critical information (Fogleman, 1995). This means that information can be directly attacked. Information attack is defined as, "those activities taken to manipulate or destroy an adversary's information or information systems without necessarily changing visibly the physical entity within which it resides" (AFDD 2-5, 1998:15). It further purports, "Manipulation of databases or parameters of reporting systems can cause incorrect information to influence leaders' decision making or destroy the adversary's confidence in its information systems" (Ibid). It follows that this is also the case with Air Force information systems. Such vulnerability is detrimental to IA. Reaching and

maintaining IA requires security from the physical, to network, and to individual user levels.

The Air Force approaches network security much like it does perimeter security for Air Force bases; allow authorized traffic and deny all else. Firewalls function as gate guards by allowing authorized traffic through ports. A firewall is a system or device designed to keep outsiders from accessing a network (Anonymous, 1998). Intrusion detection systems (IDSs) function as both gate guards and alarm systems. Just as gate guards must be trained on who is allowed on an installation, so must IDSs and firewalls be programmed for what to accept and what to block. The main problem with these systems is that there are more vulnerabilities and exploits than any one IDS can detect or firewall can block.

High sensitivity settings of IDSs and firewalls are one such vulnerability. For instance, an IDS programmed to detect numerous common system exploits, such as particular complete or partial attack signatures, will generate numerous alarms, or "false accepts and false rejects" (Denning, 1999:362). This can prove to be a vulnerability for two reasons. First, an IDS generating too many false alarms may cause administrators to ignore alarms, and potentially miss an actual incident. Second, high sensitivity settings on an IDS will cause it to slow down. If firewalls, along with IDSs, are sensitive, they will slow down network traffic, potentially causing bottlenecks throughout a network. Bottlenecks can cause traffic to surpass firewall capacities, cause them to crash, and create doors into the network for unwanted and unauthorized users. With regard to IDSs and firewalls, it is necessary to point out that from a macro view, the hardware components of network security are mostly concerned with entry into the network, and

the transmission of data. Data integrity checks may or may not be performed, but only at the bit level. The components do not examine data for meaning and content – hence, information.

Network security is geared towards protecting computer networks and information from unauthorized access; it does not guarantee protection from information corruption. Protection from information corruption must be provided by other means. Joint Publication 3-13 discusses Information Operations (IO) attack detection. Elements such as "Information Warfare Centers", "Information Systems Developers", and "Information Systems Providers and Systems Administrators" primarily address network security (JP 3-13, 1998:III-10). One element, "Information and Information Systems Users", however, relates to avoiding information corruption; more to the point, it addresses manipulated information due to deception:

> Users should be aware of potential threats to and vulnerabilities inherent in information systems. This includes recognizing abnormalities or unexplained changes in content or disturbed information and employing procedures for reporting incidents and safeguarding evidence" (JP 3-13, 1998:III-10).

Research Applicability to the United States Air Force

It should be evident from the background provided thus far that information manipulation within information systems is worthy of critical concern for the United Stated States Air Force. The Air Force relies heavily upon information technology, from day to day to strategic operations. Decision makers use information to make decisions in all facets of the Air Force. Corrupt or manipulated information can be directly or

indirectly detrimental to Air Force operations. The Air Force endeavors to protect its critical information from deception at the physical and computer network levels. There is now a call to look at a key component to the protection of critical information: the users of the information systems upon which the Air Force relies.

Problem Statement

Although JP 3-13 calls for deception detection, it is uncertain if users can do so successfully. JP 3-13 asks for users to be able to detect deception as an adversary via information systems employs it. There is little research in support of this area. Biros studied the influence of McCornack and Parks' (1986) truth-bias on perceptions of trust in "artifact produced information"; overall, results showed that participants of the study were trusting and easily deceived (Biros, 1998). An artifact is defined as, "An object, as a simple tool, produced by human workmanship" (Webster's II, 1984:42). In this study, artifacts, particularly information artifacts, are "computer- and communications-based information systems" (Zmud, 1990:97).

Most research on deception detection centers on interpersonal communication; specifically, if a receiver can accurately detect a sender's deceptive message. For instance, Buller and Burgoon (1996) discuss interpersonal deception theory (IDT) and introduce a model involving "interpersonal communication, nonverbal behavior, message processing, credibility, and deception" (Buller and Burgoon, 1996:204). Other researchers, such as Vrij and Semin (1996), Forrest and Feldman (2000), and Ekman

(1985), focus on nonverbal behaviors, such as involuntary gestures, as clues to deception detection in their research. Information Manipulation Theory (IMT) looks at deceptive messages "in terms of how the information that interactants possess is manipulated within the messages that they produce." (McCornack, 1992:1). Studies by Bavelas, Black, Chovil, and Mullett (1990) show interest in message content. Levine and McCornack (1991) assert that moderate levels of suspicion increase a person's accuracy in detecting deception.

If the Air Force is to achieve and maintain Information Superiority and Assurance, then the gray area of human-artifact deception must be explored. The studies referenced above may provide avenues to do so. However, to reach an understanding of the issue at hand, it is necessary to define a scope to begin studying.

Research Questions

Given the elements that 1) deception can occur via direct manipulation of information within an information system, and 2) little research on human to artifact deception detection exists, the following research questions are presented:

1. **Can information artifact users detect deception within artifact-produced information?**
2. **Can information artifact users be trained to improve their detect deception abilities regarding artifact-produced information?**

The following chapters explore if information artifact users can detect deception within artifact-produced information. Specifically, it will study if users can be trained to

do so. Chapter 2 will review existing literature in attempt to transform mechanisms used in interpersonal deception detection into mechanisms for user detection of deception in artifact-produced information. Chapter 3 will describe the experiment and training program used to study the research questions at hand. Chapter 4 will present the results of the research. Chapter 5 will discuss conclusions drawn from the study, as well as the limitations. Implications for the Air Force are also discussed. Since research in human-artifact deception detection is sorely lacking, a primary goal of this study is to lay the foundation for future research.

II. Literature Review

The Nature of Deception

Miller and Stiff (1993) believe that due to the limitation of human memory, communication exchanges tend to be synoptic; individuals usually provide outlines or highlights of situations rather than give second by second accounts. Excluding minutia from conversation normally is not perceived as lying or deception, and neither are informational errors nor "honest slipups" (Miller and Stiff, 1993:18). Furthermore, "virtually all communicative exchanges are marked by the omission of information" (Ibid). Even so, Miller and Stiff believe that absolute veracity within interpersonal communication is not realistic and contend that deceptive communication will occur at some point within personal relationships. The question then becomes when, assuming that omissions of information will occur, are communicative exchanges considered deceptive? "Selective and oversimplification are usually not considered deceptive unless the message recipient has reason to suspect the message source of duplicity" (Ibid:18).

According to Webster's II New Riverside Dictionary, *deceive* is, "to mislead or delude" (p. 183). Ekman (1985) writes that lying or deception occurs when, "one person intends to mislead another, doing so deliberately, without prior notification of this purpose, and without having been explicitly asked to do so by the target" (Ekman, 1985:28). A simpler definition of deception is, "a message knowingly transmitted by a sender to foster a false belief or conclusion by the receiver" (Burgoon, Buller, Guerro,

Afifi, and Feldman, 1996:51). These definitions of deception suggest some common threads among them: a sender with intent to mislead, an unsuspecting receiver, and false or misleading information. "Thus, to be considered potentially deceptive, communicative exchanges must involve perceptions by one or more of the involved parties of *intent to deceive*" (Miller and Stiff, 1993:19, emphasis in original).

Researchers also offer different types of deception. Ekman (1985) states that concealment and falsification are the two primary ways to lie or deceive. He found that given a choice, liars will choose concealment rather than falsification because nothing has to be made up, there is less chance of inconsistencies, and it is easier to cover afterward if discovered. Other researchers consider equivocation, simply stated as intentionally evasive language, as another classification of deception (Burgoon, Buller, Ebesu, and Rockwell, 1994:305). Bavelas et al (1990), however, do not consider lying as equivocation. Their position is that equivocation is neither a false message nor a clear truth; both true and false messages may be clear or equivocal. They contend that there are different degrees of falseness.

Interpersonal Deception

In general, humans are poor lie detectors, and "are only slightly more accurate than the flip of a coin when making judgments of truth and deception" (Miller and Stiff, 1993:69). As such, interpersonal deception research is abundant. Interpersonal communication is at the core of this research, particularly face-to-face communication. Many researchers look at nonverbal aspects of communication for clues to deception

(Ekman, 1985, Feeley and deTurck, 1995, Buller and Burgoon, 1996, Vrij and Semin, 1996). Nonverbal aspects of communication include facial expressions; involuntary/unconscious body movements, etc. (Ekman, 1985). Buller and Burgoon labeled such "inadvertent behavior" as "non-strategic" (Buller and Burgoon, 1996:207). Ekman, in explaining why lies fail, theorized that the stronger and greater the number of emotions, the more difficult it is to conceal them, which will likely lead to behavioral "leakage" (Ekman, 1985:21).

Studies in interpersonal deception detection typically employ experiments which have observers watch videotapes of communicators making statements and judge the veracity of the statements; the experimenters will either gather results in terms of accuracy, or they will analyze what clues the observers used to make their judgments (e.g., deTurck, 1991, Vrij, 1993, Vrij and Semin, 1996). There is a potential flaw with this approach; most deception research focuses on face-to-face interaction, but the methods used are non-interactive in nature (Buller and Burgoon, 1996).

Other approaches to interpersonal deception detection address the contextual aspects of communication, primarily the verbal messages themselves. Bavelas et al, with regard to detecting equivocation and/or deception, state that the best approach "...is to pay extremely close attention to both the situation and what is said" (Bavelas et al, 1990:176). They purport that communication always involves sender, content, receiver, and context. Ambiguity along any or all of the four elements within a message indicates equivocation. Two dominant theories that serve as frameworks for deception detection are Interpersonal Deception Theory, or IDT, (Buller and Burgoon, 1996) and Information Manipulation Theory, or IMT (McCornack, 1992). IDT looks at both the interpersonal

and contextual aspects of communication, while IMT focuses on message design. Both theories are discussed below.

Interpersonal Deception Theory

Buller and Burgoon developed IDT as "a merger of interpersonal communication and deception principles designed to better account for deception in interactive contexts" (Buller and Burgoon, 1996:203). IDT possesses several key attributes and assumptions associated with both interpersonal communication and deception.

Interpersonal Communication Attributes and Assumptions. IDT assumes interpersonal communication is a dynamic activity between a sender and a receiver; neither is a passive participant. IDT also assumes that interpersonal communication is goal-oriented, such that there are strategic and non-strategic behaviors involved. Behaviors are strategic in that senders and receivers both must simultaneously encode and decode messages during dynamic interactions. Non-strategic behaviors, typically unconscious or unintentional, which often accompany strategic behaviors, are manifested in emotions, nervous movements, etc. Another key attribute of communication is that messages are judged on credibility. Credibility is defined as "a constellation of judgments that message recipients make about the believability of a communicator" (Buller and Burgoon, 1996:207). In IDT, credibility encompasses character, competence, composure, sociability, and dynamism.

IDT recognizes that interpersonal communication is a complex process and places heavy cognitive demands on communication participants. This is because participants

must act as both sender and receiver as they exchange messages, meanwhile attempting to ensure messages are credible. This makes it necessary for participants to become "selective information processors" in order to successfully encode and decode messages (Buller and Burgoon, 1996:208). IDT assumes that those with greater social skills are better equipped to handle communication demands.

Along with cognitive demands are expectations and norms held by communication participants. In general, people form a truth-bias (discussed later in this chapter), such that they expect that what others tell them during interpersonal exchanges is true. This, in turn, attaches trust to interpersonal communication: "Trust is the foundation on which enduring relationships are built, and trust grows with the belief that another is communicating in an honest, straightforward manner" (Buller and Burgoon, 1996: 209). Because expectations exist, this implies that such expectations might not be met. Then, "Interactants recognize violations of expectations, violations prompt an attentional shift to the communicator and the violative act, and violations activate an interpretive and evaluative appraisal process" (Ibid). It is in this state that deception becomes manifest.

Deception Attributes and Assumptions. IDT assumes that deliberate information management is a key facet of interpersonal communication (Buller and Burgoon, 1996). Generally, people select what information they will hide, obscure, avoid, or fabricate. They do so by encoding their messages such that the dimensions of veridicality (veracity), completeness, directness/relevance, clarity, and personalization are altered in some way (Burgoon et al, 1996). *Veridicality* refers to the truthfulness of information, which can be broken down into *actual* and *apparent*, or objective vs.

perceived. *Completeness* refers to the proper amount of information being present in a conversation. *Informational* and *conversational* completeness are also objective vs. perceived elements; only the sender knows if the necessary information is present whereas the receiver perceives the information present is sufficient. *Directness/relevance* refers to messages being *semantically* (content) relevant or *syntactically* (grammatically) relevant. *Clarity*, in general, refers to the level of equivocation present in a message. *Personalization* means "utterances are presumed to belong to those who utter them. Violating this basic assumption can mislead receivers" (Burgoon et al, 1994: 53-55).

A deceptive message in IDT generally is comprised of the central deceptive message, ancillary messages, and inadvertent behaviors. Ancillary messages enhance the appearance of truthfulness of central messages or "protecting the source" if deception is detected (Buller and Burgoon, 1996: 209). Inadvertent behaviors, as previously mentioned, are typically nonverbal in nature. Of the three deceptive message elements, inadvertent behaviors are "functionally" opposite from the other elements, such that they are most likely to detract from the apparent credibility of deceptive messages (Ibid).

Finally, IDT posits that deception will place cognitive and emotional demands, above and beyond those associated with normal communication, on both deceivers and detectors. Deceivers may experience detection apprehension (fear of being caught), while trying to give the outward appearance of a calm and truthful demeanor as well as maintain their deception by continuing to encode messages as appearing truthful. Deceivers must also gauge detectors' detection abilities and adjust their deceptive strategies accordingly. The cognitive and emotional demands on detectors are "due to their motivation to detect deception, heightened surveillance, cognitive difficulty, and

unpleasantness associated with uncovering duplicity" (Buller and Burgoon, 1996: 210). As outlined above, IDT addresses both the nonverbal and contextual aspects of interpersonal communication with regard to deception. Information Manipulation Theory (McCornack, 1992) ignores nonverbal communication and focuses instead on message design.

Information Manipulation Theory

McCornack (1992) introduced a theory that suggests that, during communication with others, individuals form deceptive messages by manipulating the information within them along certain dimensions. Unlike IDT, nonverbal cues do not factor into Information Manipulation Theory (IMT). The central foundation of IMT is built upon Grice's (1975) Cooperative Principle (CP) and conversational maxims. The CP maintains that, during conversations, individuals generally adhere to unwritten conversational rules: "Make your conversational contribution such as is required, at the stage at which it occurs, by the accepted purpose or direction of the talk exchange in which you are engaged" (Grice, 1975:45). The CP results in four maxims on which individuals base their conversations: quality, quantity, relation, and manner. IMT is rooted in the CP maxims. Specifically, "messages that are commonly thought of as deceptive derive from covert violations of the conversational maxims" (McCornack, 1992:5). The description of each maxim is outlined below.

Quality. Quality pertains to the veracity of information within a message. Unless given reason to believe otherwise, interactants generally assume what they are

told by the other is true. Deception can occur when an individual intentionally and covertly inserts false or misleading information, appearing to be true, into his or her messages. The deception is successful if the receiver of the message believes it at face value.

Quantity. Quantity relates to the amount of information contained in messages. Individuals generally expect that their communication partners are providing an adequate amount of information in a given exchange. A sender of a deceptive message may either provide too much information or omit important information in an attempt to direct a receiver's perceptions in a particular direction. Intentionally providing too much information may serve to distract the receiver of the message or confuse the issue at hand. Alternatively, a sender may not wish the receiver to know the true status of a situation, and thus may omit pertinent information.

Relation. Relation pertains to the relevance of information within messages. Individuals generally assume that the information provided to them is relevant to the context of the situation. Similar to providing too much information, a deceiver can insert irrelevant information into a message to distract the receiver from the actual topic at hand. Such information can even be true, but of no value since it is irrelevant.

Manner. The maxims of quality, quantity, and relation pertain to what information is said or provided; manner pertains to how it is said or provided. Generally, individuals should, "present information in a brief and orderly fashion" and avoid obscurity and ambiguity (McCornack, 1992:5). Information presented in a sarcastic or ironical fashion can shape an individual's perceptions in particular ways. A deceiver also purposely may gloss over an important detail to make a receiver perceive it as

insignificant, potentially causing the receiver to not take a necessary action related to the detail.

The CP and its associated maxims outline how communication exchanges are generally formed. IMT delves into the maxims and attempts to address what happens when they are not adhered to in message exchanges. IMT recognizes that messages can be deceptive along one or more of the dimensions of quality, quantity, relation, and manner. IMT was not developed to create categories for deception types, but rather, "as a descriptive tool for addressing particular messages" (McCornack, 1992:15).

As Chapter 1 points out, deception is not limited to the realm of interpersonal communication. Heavy reliance on IT has opened the door to a more unique type of deception, which is artifact-based deception. Its uniqueness stems from the absence of nonverbal cues. Whereas interpersonal deception is based on human-human interaction, artifact-based deception, as described in this study, will focus on human-artifact interaction. The literature review thus far has looked at interpersonal deception as a possible bridge to understanding and identifying artifact-based deception. The following sections turn to the artifact side of the issue.

Artifact-Based Deception

Zmud (1990) wrote an article on the effects of new technologies on strategic information behaviors, primarily those of managers within organizations. Although the article was "based far more on informed speculation than on an empirical understanding", eleven years later its message is not just a plausibility but also a reality (Zmud, 1990:

113). According to Zmud, "individuals do engage in the deliberate misrepresentation of information or restriction of access to information in order to influence the behaviors of others" (Ibid:95). He pointed out that a principal problem for most managers, particularly with the information capabilities that IT provides, is an overabundance of information. Managers, in an effort to avoid information overload, will delegate their information processing responsibilities, whether it is to other individuals or to information artifacts with processing capabilities. The more that managers do this, "the more susceptible an individual is to the strategic information behaviors of others (Ibid:109). Generally, the farther removed from information a manager becomes, the better chance for misrepresentation of information by others. Use of IT to store organizational information and transactions poses another problem: "stored histories of managers' information processing behaviors provide exceptional guides as to how best to present misrepresented information to a particular individual" (Ibid:110).

Zmud (1990) considered technology as neutral and that technology itself would not affect the strategic information behaviors of others. It was any individual skilled in the inner workings of technology who could potentially use it to misrepresent information or manipulate the strategic information behaviors of others. Although Zmud focused his article on the strategic information behaviors of managers, it is not a grand logical leap in applying similar rationale of the effects of IT on any information artifact user. The next section discusses how trust plays a role in why individuals are deceived in both interpersonal relationships and human-artifact interactions by drawing parallels between truth-bias and automation bias.

Truth-bias

McCornack and Parks (1986) introduced the concept of truth-bias to interpersonal deception research. They found that as relationships, particularly romantic ones, develop, individuals' abilities to accurately detect deception decrease. McCornack and Parks theorized that judgmental confidence and truth-bias acted as intermediating variables. As a relationship develops, an individual's confidence in his or her ability to discern a partner's truthfulness increases. As this confidence increases, the more individuals presume that partners are truthful. McCornack and Parks found empirical support that since such presumptions preclude reasons to believe otherwise, individuals will not likely detect deception by their partners. A replication study done by Levine and McCornack (1992) generated similar support.

In order to understand the parallel between truth-bias and automation bias, it is necessary to look at a fundamental factor of both constructs; trust. The next section will begin by describing a dominant taxonomy of interpersonal trust, and then the transition from interpersonal to human-machine trust.

Interpersonal Trust. Research shows that there is little agreement as to a common definition of trust. Barber (1983) found that although no agreement seems to exist, there are certain elements that are common to most definitions. He used the common element of expectation to develop a taxonomy of interpersonal trust.

Barber found that there are three types of expectations that constitute trust: persistence, technical competence, and fiduciary responsibility. Persistence relates to the expectation of "fulfillment of the natural and moral social orders" (Barber, 1983:9). An

example of this expectation is that people trust the sun will rise and set each day. Technical competence may consist of "expert knowledge, technical facility, or everyday routine performance" (Ibid:14). In a doctor-patient relationship, a patient trusts that the doctor, by nature of the profession, is technically competent. Fiduciary responsibility pertains to the "moral dimension of interaction" (Ibid:15). It most often is associated with positions of authority or power, such as government officials, professionals, etc. In general, individuals in such positions are expected to put the interests of those they are serving before their own; they are expected to not abuse their power.

Interestingly, Barber states, "We may usefully think of these various kinds of trust as existing not only between individual actors but also between individuals and systems – indeed, even between and among systems" (Barber, 1983:18). Barber was referring to systems in terms of legal, educational, and medical organizations as a whole when he made the statement. The use of the term system makes it reasonable to assume that trust between an individual and a machine or artifact as a system would also apply, as seen in Muir's research.

Human-Machine Trust. Muir (1987) explored the possibility of parallels between human-human trust and human-machine trust. At the time of the study, no models for human-machine trust existed. Using Barber's (1983) taxonomy of interpersonal trust as a basis, Muir proposed such a model. The persistence aspect of trust with regard to machines "allows us to construct rule bases for decision support systems" (Muir, 1987:529). The primary expectation of trust between humans and machines is technical competence. Humans can expect machines to perform the technical tasks for which they were designed and nothing beyond. For example, a

machine designed to only collect data will not be expected to analyze or interpret it. When the technical competence of a machine exceeds that of a user, it can be said that the machine holds power, and the user gives over his or her trust to the machine. Fiduciary responsibility, with regard to the machine, means that the user trusts that the machine will not abuse its power and will carry out its role.

Automation Bias

Automated systems were introduced to the work environment with the goal of reducing human error. Skitka, Mosier, and Burdick (1999) argue that although human error may be reduced in specific areas, different classes of errors occur. They found that as human operators rely more on automation, more errors of commission or omission by operators occur. Operators may commit errors of omission when, despite non-automated evidence, they do not take action in a particular situation because the evidence was not presented by the automated system. Errors of commission occur when operators take action based on information an automated system is providing them, despite other reliable sources instructing it would be imprudent to do as the system directs. Examples of this have occurred in real-life situations. Aviation accidents have occurred because pilots blindly trusted automated components within their aircrafts, without monitoring the components. In one instance, Soviet fighters shot down an aircraft because the magnetic heading the pilots programmed was inaccurate (Skitka et al, 1999). In another instance, a plane crashed because the crew believed that they were holding a certain altitude but

failed to notice that the autopilot mechanism had accidentally been disengaged (Skitka et al, 1999).

Skitka et al's (1999) study supports that of Muir's (1994) human-machine research. Muir assumes that if humans could not build automation that can be trusted, then it would not be built at all. Allowing a system to automate a process exhibits trust. Muir found that the more operators trust automation, the less they will intervene with the automation's control. This has the potential to cause an operator to be unaware of automation failures or errors. This is particularly true if the technical competence of the machine far exceeds that of the operator: "If the automation fails in an area outside the supervisor's knowledge base, the supervisor will fail to detect the fault, and fail to override the automation" (Muir, 1994:1907). Conversely, if an operator's trust drops below a critical point, then he or she will intervene manually with the automation. Moray, Hiskes, Lee and Muir (1995) found that the first time a system proved unreliable, operators doubt themselves rather than the system. Only after repeated errors will operators finally attribute the failures to the system.

As seen above, parallels can be drawn between truth-bias and automation bias. As relationships develop positively between people, they tend to regard each other as truthful. They are also confident that they would be able to detect deception by the other if it occurred. However, as research shows, this is generally not the case. People tend to trust automation. The more they trust automated systems, the less they intervene with its operation, thus resulting in automation bias. When the technical competence of the automation exceeds that of the operator, coupled with the level of operator trust, operators are less likely to recognize automation errors or failures when they occur. This

is not to say that automation error or failure should be equated with deception. However, it can be inferred that someone with high technical competence, other than an operator, can intentionally interfere with or manipulate automation to cause it to commit errors or fail. Then, it may be considered deception on the part of the manipulator, in which the deception is successful if the operator does not detect it.

Deception Detection Training

Plentiful documentation exists supporting the fact that people, primarily in the interpersonal arena, deceive each other. They are able to do so because people are generally poor deception detectors. There is little solid research addressing artifact-based deception. Zmud (1990) shows that people perform strategic information processing behaviors. He also offered a convincing argument that, with growing reliance on information artifacts, such behaviors have the potential to be deceptively manipulated. Zmud's argument holds even more logic and clout, given that it is possible to directly alter and manipulate information within systems without changing the appearance of the systems. Although the logic and likelihood of human-artifact deception exists, there is a lack of empirical support.

This state of affairs raises the question: can people be trained in deception detection? Research on the interpersonal side of the issue is inconsistent. Literature shows most focus on the use of nonverbal cues to detect deception. One element in the study of nonverbal cues is perceived versus actual indices of deception. Vrij (1996) found that unreliable cues such as nervousness, avoidance of eye contact, and an increase

in hand and foot gestures were perceived by most people as reliable cues of deception. Even when trained that deceivers actually tend to decrease movement during deception, judges still generated low accuracy results. Forrest and Feldman (2000) placed judges in low and high involvement conditions where they judged the veracity of verbal statements. Those in the low involvement condition were trained in the more reliable indices of nonverbal cues and were instructed to focus on them while judging. The high involvement condition subjects were instructed to focus on the verbal message itself. Those using the peripheral route, the low involvement group, had higher accuracy rates than the high involvement condition. Zuckerman et al (1984) found that judges' accuracy was better when they received feedback on their veracity judgments. Feeley and deTurck (1997) used case-relevant and case-irrelevant information to develop baseline behavioral information. Case-relevant focused on questions related to a staged investigation, and case-irrelevant focused on non-related information such as name, age, and occupation of the target to be judged. They found that case-relevant information in conjunction with attending to nonverbal cues seemed to enhance detection accuracy, but not much.

Mentioned earlier, literature specific to human-artifact deception detection training is overwhelmingly slim. Biros (1998) found that users' abilities to detect deception in artifact-produced information are limited. In his study, user experience and state suspicion, not training, significantly improved deception detection. Finally, due to the complexity of information artifacts, developing a training program in deception detection would prove difficult.

Muir discusses the calibration of trust in machines. She states, "It is inappropriate for operators to trust all automation equally, or all functions or components within a

single machine equally. The operator's task is to adjust or calibrate their trust to the true properties of each specific referent and then to use it accordingly" (Muir, 1994:1918). The goal would be to avoid trusting and using poor automation, or to avoid not trusting good automation when appropriate. Coupling calibration of trust in machines with the construct of automation bias theoretically makes it possible to avoid errors of commission and/or omission, due to operators better understanding the machines they use. Granted, Skitka et al (1999) did not discuss errors in terms of deception. However, it is worthy to investigate if calibration of trust in machines, extending to information artifacts, and assuming such calibration would lead to better user understanding of systems, would lead to better artifact-based deception detection.

Klein and Goodhue (1997) challenge "earlier assertions that humans are, in general, poor error detectors" (Klein and Goodhue, 1997:1-29). They conducted a study that generated results suggesting that error detection as an explicit goal paired with incentive structures can have an effect on error detection. As with Skitka et al (1999), the focus of the study was not on intentional (deceptively introduced) data errors, but the results of Klein and Goodhue's study suggest an incentive structure might positively influence information artifact users' deception detection abilities.

Suspicion is an element worth mentioning, although this section addresses training. McCornack and Levine (1990) introduced the notion of three types of suspicion that can influence deception detection accuracy. A predisposition towards considering others' communication as suspect is labeled generalized communicative suspicion (GCS). Specific contextual clues alerting one to possible deception is labeled as state suspicion. The third type of suspicion, the conceptual opposite of truth-bias, is a "judgmental bias

toward processing all of a partner's messages as lies" (McCornack and Levine, 1990:220). They found that moderate levels of suspicion (i.e., GCS and state suspicion) enhanced deception detection accuracy. Burgoon et al (1994) and Toris and DePaulo (1985) found contrary results. Toris and DePaulo state, "Increased suspiciousness, in and of itself, served only to destroy the confidence of both perceiver and perceived in their own interpersonal skills, and to erode their trust in each other" (Toris and DePaulo, 1985:1071). Their results showed that primed interviewers were no more accurate than naïve interviewers at deception detection.

Studies involving suspicion agreed upon one area. This is that there seems to be a fine line where suspicion can have a positive effect on deception detection. McCornack and Levine (1990) suggested moderate levels of suspicion could enhance deception detection. However, in agreement with Burgoon et al (1994), high amounts of suspicion in individuals proved counterproductive such that they ended up developing a lie-bias. This, combined with Biros' (1998) finding of decreases in productivity of information artifact users, may suggest that inducing suspicion overall can have undesirable effects.

Piecing the Puzzle Together

Research surrounding interpersonal deception detection poses potential difficulties for the study at hand. Artifact-based deception is unique from interpersonal deception detection. Nonverbal cues are at the core of interpersonal deception detection; however, there are no such cues associated with human-artifact interactions. Therefore,

the nonverbal cues aspect must be removed from the exploration of human-artifact deception detection.

IDT and IMT seem to offer similar qualities that are independent of nonverbal channels of communication that could contribute to artifact-based deception. IDT includes dimensions of veridicality, completeness, directness/relevance, and clarity. These are very similar to the IMT maxims of quality, quantity, relation, and manner. The attributes of both theories address the content and context of messages. Theoretically, these attributes can be applied to assessing the veracity of artifact-produced information. The following assumptions will be made for the remainder of the study:

1) The IMT maxims are more applicable to the understanding of the current issue, and thus will be central to the remainder of the study.

2) The calibration of trust will be considered analogous to training on an information artifact.

This study used a Command and Control (C2) battle environment simulation game as an information artifact within an exploratory experiment. Although all four IMT maxims are assumed central to the study, only those of quality and quantity were manipulated in the experiment. This was because it was easier to operationalize and quantify the maxims of quality and quantity in the given environment, which will be outlined in subsequent chapters.

This literature review demonstrated that people can be deceived through artifact-based deception. It also discussed deception detection theories that use context-based detection methods in discerning deception. Based on these notions, the assumptions

made, and the information system chosen for the study, the following propositions are proffered:

P1: Information artifact users trained in both the quality and quantity maxims will perform better than information artifact users not trained in any context-based deception detection methods.

P2: Information artifact users trained in the quality maxim will perform better than information artifact users not trained in any context-based deception detection methods.

P3: Information artifact users trained in the quantity maxim will perform better than information artifact users not trained in any context-based deception detection methods.

P4: Information artifact users trained in both the quality and quantity maxims will perform better than those trained in the quality maxim alone.

P5: Information artifact users trained in both the quality and quantity maxims will perform better than those trained in the quantity maxim alone.

Chapter 3 justifies why the above propositions are labeled as such, rather than as hypotheses. The next chapter also describes the initial endeavors to obtain empirical support for the propositions in a laboratory setting.

III. Methodology

Introduction

Chapter 1 identified the need for research human-artifact deception detection and its applicability to the United States Air Force. Chapter 2 explained how specific research is lacking, leaving the area wide open for multiple avenues of study. Chapter 2 drew from theories in interpersonal deception detection to develop a foundation and initial propositions for human-artifact deception detection. This chapter describes the methods and procedures used to test the propositions stated in Chapter 2.

Information Manipulation Theory (IMT) is a theory of interpersonal deception detection that is of particular interest to this study. IMT focuses on message design, rather than on the nonverbal cues associated with communication. IMT posits that information can be manipulated along the dimensions of quantity, quality, relation, and manner (McCornack, 1992). Although all four of these dimensions are important, only the dimensions of quality and quantity were operationalized in the experiment described in this chapter. The quality and quantity dimensions allowed for empirical data to be gathered to support or disconfirm the stated propositions.

Experimental Design

Figure 1 shows the research design for the experiment used in this study. This represents a pretest-posttest, control group design, which is considered a true experiment. True experiments offer the highest internal validity of research designs (Dooley, 1995).

$$\begin{array}{cccc} & O & X_{QQ} & O \\ R & O & X_{QL} & O \\ & O & X_{QN} & O \\ & O & & O \end{array}$$

Figure 1. Research Design

This experiment used four experimental groups. The pretest and posttests were each 20-minute computer simulations. The treatment (represented by X_{XX}) was a brief training program covering the IMT maxims of quality, quantity, or both. This training was applied to the treatment groups between simulations. The subscripts on the *X*s indicate which variation of the training was applied: *QQ* denotes both quality and quantity, *QL* denotes quality-only, and *QN* denotes quantity-only. The fourth group acted as the control group, thus receiving no treatment.

Subjects were randomly assigned to treatments. Several timeslots were available for subjects to participate during the one week of data collection. In addition, each session had a four-subject capacity; for example, one session could represent four subjects receiving the quality-only treatment.

Subjects

Thirty-two subjects were taken from a pool of AFIT graduate students. Included in the subjects were two civilians and two international students. Subjects were told they would be testing a prototype for a C2 battle environment simulation. As motivation for participating in the experiment, all subjects were entered into a random drawing for a $25 gift certificate for Pizza Hut. Several students also received extra credit from an instructor for their participation.

A power analysis for a one-way Analysis of Variance (ANOVA) was conducted (Lenth, undated) to determine how many subjects were needed in each group to achieve sufficient power. The power of a test is the probability that the results obtained are correct. Based on this analysis, subjects were divided into groups with seven subjects in the *QQ* group, nine subjects in *QL* group, eight subjects in the *QN* group, and eight subjects in the control group. The Table 1 shows the power analysis results and verifies that the subject numbers within each of the groups achieved significant levels of power.

Table 1. Power Analysis for One-Way ANOVA, 4 Levels

N	Power	Alpha
10	.9959	.05
9	.9908	.05
8	.9797	.05
7	.9568	.05

Instruments

The data collection tool used in this study was a highly modifiable, simulation-based program developed by the Aptima Corporation called the Distributed Dynamic Decision-making system (DDD). Subjects using the program could be introduced to several different military-related situations. The DDD is capable of operating on several computer platforms, with Redhat Linux 6.0 used for this study. All scenarios used in the program were scripted and coded into the system. The scenarios used in this experiment were modifications of scenarios developed by Fields (2001) and Langhals (2001).

The scenarios used for this study required subjects to play the role of air defense commanders deployed to a hostile foreign situation. The same potential real-world scenario created and used by Fields (2001) was used for this experiment as well (Appendix A). Subjects were asked to identify aircraft entering their assigned battle space based on information received through radar and network reports. Subjects then had to decide whether to allow the aircraft into the airspace or shoot it down. In addition, they were asked to report any discrepancies in information provided to them.

This experiment required subjects to be trained on the use of the DDD. This training was distinct from the experimental treatment, and was not itself considered a manipulation. The training served to educate subjects on the DDD functionality and scoring, as well as make them aware of the different sources of incoming information that would be key to the experimental manipulation. Subjects were advised that they had direct links with radars and were also a part of a Wide Area Network (WAN). They were informed of the possibility of information warfare attacks, such as delay of service,

network crashing, or information manipulation. Refer to Appendices B and C for the DDD training script and slides.

Three questionnaires were used in this experiment. The first questionnaire collected two types of information. The first part asked for subject demographics (summarized in Appendix D). The second part of the questionnaire contained a seven-item, Likert-like scale measuring beliefs about computers. The questionnaire was modified from a one used to measure interpersonal trust to instead measure human trust of computers (Fields, 2001). Given that this experiment involved human-artifact relationships and used the same computer program as the Fields (2001) study, the computer belief information was collected as well in case it was found that trust affected the results. Refer to Appendix E for the participant information/computer beliefs questionnaire.

The second multiple-choice based questionnaire measured the effectiveness of the DDD system training provided before the first simulation (Fields, 2001). This questionnaire was given to all subjects in all groups (Appendix F) immediately after the hands-on training demonstration. The third and final questionnaire was also multiple-choice, containing two generic questions about the DDD system and other questions pertaining to the training received during the treatments between the first and second simulations. This was administered immediately after the treatment, prior to the start of the second simulation. There were three variations of the third questionnaire, one for each of the *QQ*, *QL,* and *QN* groups. The control group did not complete the third questionnaire since they did not receive any treatment. The variation was a simple omission of questions that did not pertain to a particular treatment. For example, the *QQ*

questionnaire contained the generic questions and the questions regarding quality and quantity. The *QL* questionnaire, however, contained the generic and quality questions from the *QQ* questionnaire only, and likewise for the *QN* questionnaire. Refer to Appendix G for the full version of the third questionnaire given to the *QQ* group.

Pre-pilot and Pilot Studies

Pre-pilot and pilot studies were conducted to solidify the experimental procedure. The pre-pilot study used one subject who went through the DDD system training as well as the experimental manipulation of the *QQ* group. The subject completed all the appropriate training questionnaires and the answers indicated that the questions reflected what was trained. Recommendations from the subject regarding minor procedural changes were incorporated into the experimental script.

A pilot study was then conducted, using one subject for each of the experimental groups. It was already determined that experimental sessions would each take at least one and one-half hours. Therefore, the pilot study's chief purpose was to provide manipulation checks of the treatment questionnaires and to ensure smooth experimental execution. Table 2 below is a summary of how pilot study subjects in the experimental groups performed on the contextual training questionnaires. The results suggested that the questions developed measured what was intended; therefore, they were deemed suitable for use in the main experiment. Feedback from subjects indicated that use of the discrepancy button should be clarified in subsequent experimental sessions. This clarification was incorporated into the experiment script.

Table 2. Pilot Study Manipulation Checks (Training Questionnaire Results)

Group	Number Correct	Total Possible	Percentage Correct
QQ	5	6	83.3
QL	4	4	100
QN	4	4	100

Experimental Procedure

Fourteen DDD sessions were conducted over a five-day period. Subjects were assigned numbers when they entered the experiment room to ensure anonymity. They were initially seated at a table where they were asked to read and sign an informed consent form (Appendix H) and to complete the participant information and computer beliefs questionnaire. Subjects then were asked to follow along with overview slides provided to them as the experimenter read from the DDD training script.

Once the main portion of the training script was read, subjects were then placed in front of a DDD computer for a hands-on training demonstration. The forms filled out at the start of the experiment were annotated with subjects' numbers and placed in large envelopes next to the subjects' respective stations. The experimenter then continued with the training script, guiding the subjects through the tasks they would be performing during the full simulations. This allowed them to become familiar with the DDD and to ask any questions they had about how to play the game. Tasks included getting information on an asset, assigning confidence intervals, attacking tracks, and reporting discrepancies if they detected inconsistencies between what they saw on their battle space display and the information received from the radars and over the network. Reference

slides covering the scoring system, network participants, and track icons were provided at all of the DDD stations. Once the subjects had practiced performing the requested tasks, they used the remaining time to practice on their own and ask any questions until the end of the training simulation. The hands-on portion of the demonstration and practice ran for approximately ten minutes. Subjects were asked to complete the DDD training evaluations and place them in their envelopes. They were then encouraged to take a short five to ten minute break in order for the experimenter to set up the computers for the first full simulation.

Once the first simulation was ready, subjects took their seats at their DDD stations. The experimenter then read to the subjects from the scenario brief as they read along. Subjects were told to begin the first full twenty-minute simulation, and to feel free to ask questions throughout. Upon simulation termination, individual subjects' scores were recorded. Subjects were then asked to take a ten-minute break. The experimenter used the break to load the second full simulation scenario onto all of the computers in preparation for the second simulation.

Subjects returned to their stations after the break and were asked not to start until told to do so. The treatment groups were read a script reminding them of the intense information environment that they had just encountered during the first simulation (Appendix I). They were asked to reflect on whether they had the right type and amount of information they needed to perform their assigned tasks, and if they thought they could detect deceptive information. They were then told that research indicated that people could be taught deception detection along certain dimensions. Quality and quantity dimensions were described to those in the *QQ* group, quality to the *QL* group, and

quantity to the *QN* group. All were given DDD-specific examples of how quality and quantity violations could occur, dependent upon the group they were in. An example of a quality violation was if the flight information for a particular track as reported by a directly linked radar was different than the information reported, for the same track, over the network connection. Subjects were told that one to three messages would be received per track, dependent upon which radar detected it. If a track only entered the detection zone for one radar, then only one report message would be generated. A quantity violation occurred if zero messages or more than four messages for a particular track appeared. Subjects were given the appropriate treatment questionnaire regarding the training just received, which were placed in the envelopes along with the previous questionnaires. The subjects were then allowed to begin the final 20-minute simulation. The control group received none of the treatments described above. When subjects in this group returned from their breaks after the first simulation, they were allowed to begin the second simulation once they all were seated at the DDD stations.

Scores were once again collected at the end of the simulations. The subjects were then briefed on the true nature of the study, advising them that the percentage of accurate discrepancies they reported was the true measure of their success, not the overall game scores as they were initially told. They were also told what group they were assigned to. They were given the opportunity to ask questions and provide feedback on the experiment. They were then thanked for participating, were asked not to discuss the experiment with anyone to avoid experiment bias, and were free to go. Subject log files were copied to disk for follow-on data analysis.

All information regarding scripts, questionnaires, and other training materials can be found in the appendices. Chapter 4 will present the results of the analysis conducted on the data collected. Chapter 5 will discuss these results, as well as limitations of the study. It will also address implications and suggestions for future research endeavors.

IV. Results and Analysis

Introduction

The previous chapters have presented an initial study of human-artifact deception detection. Chapter 1 described the state of affairs and identified the need for such research. Chapter 2 outlined research from interpersonal deception detection and interpersonal trust to build a foundational bridge from interpersonal to human-artifact deception detection. This generated initial propositions stating that information artifact users who are trained in contextual-based methods will possess better artifact-based deception detection skills than those who are not trained. Chapter 3 described the methodology used to gather supporting empirical results. This chapter now presents the results of the experiment.

Analysis of Variance

The measurements used to test the propositions as presented in Chapter 2 were straightforward. The methodology chapter stated that subjects' performance was judged by the percentage of accurate discrepancies that they reported during each simulation. Table 3 summarizes the means and standard deviations of both simulations by group.

Table 3. Group Means and Standard Deviations

Simulation 1				
Group	**N**	**Mean (%)**	**Std. Dev. (%)**	**Std. Error Mean (%)**
QQ	7	21.6	19.4	7.3
QL	9	7.6	9.3	3.1
QN	8	19.5	9.1	3.2
C	8	15.6	21.7	7.7
Overall	32	15.7	15.8	2.8
Simulation 2				
Group	**N**	**Mean (%)**	**Std. Dev. (%)**	**Std. Error Mean (%)**
QQ	7	17.3	13.2	5.0
QL	9	7.6	9.1	3.0
QN	8	28.0	16.9	6.0
C	8	23.2	12.6	4.4
Overall	32	18.8	14.8	2.6

Any track could have, at most, one associated discrepancy. Simulation 1 had forty-three total tracks that appeared onscreen throughout the twenty-minute simulation, with twenty-one of them having discrepancies. Simulation 2 had thirty-two tracks, with sixteen of them having discrepancies. Because all groups had received no contextual-based training, Simulation 1 served as the baseline of comparison to Simulation 2.

A one-way Analysis of Variance (ANOVA) was conducted to compare the means of all the groups within each simulation. The results in Table 4 show that there was no significant difference between the groups in Simulation 1 ($F(3,28) = 1.300$, $p = .294$). This was expected since Simulation 1 was the baseline for subjects within all groups. There was a significant difference between the groups in Simulation 2 ($F(3,28) = 3.827$, $p < .05$). This was also expected, since it initially suggested that the treatment applied

between simulations was effective. The ANOVA results for Simulation 2, however, did not indicate which groups were significantly different. This required further analysis.

Table 4. Overall Group ANOVA Results

Analysis	df	Mean Square	F	p
Discrepancies Sim 1 Overall				
Between Groups	3	.032	1.300	.294
Error	28	.024		
Discrepancies Sim 2 Overall				
Between Groups	3	.066	3.827	.021
Error	28	.017		

Tukey Honestly Significant Differences (HSD) Test

A Tukey Honestly Significant Differences (HSD) test was conducted to analyze the means of one group against each of the other groups individually for Simulation 2. The results of the Tukey HSD (Table 5) indicated two significant differences were found between the groups. One significant difference was in the opposite direction expected, while the other was an unexpected result that was independent of the propositions.

Table 5. Tukey HSD Results – Simulation 2

Description		Mean Difference (%)	Std. Error (%)	p
QQ	*QL*	9.7	6.6	.471
	QN	-10.7	6.8	.406
	C	-5.9	6.8	.822
QL	*QQ*	-9.7	6.6	.471
	QN	-20.4**	6.4	.017
	C	-15.7*	6.4	.092
QN	*QQ*	10.7	6.8	.406
	QL	20.4**	6.4	.017
	C	4.8	6.6	.881
C	*QQ*	5.9	6.8	.822
	QL	15.7*	6.4	.092
	QN	-4.8	6.6	.881

*p < .1
**p < .05

It was expected that any significant differences found would be in favor of the treatment groups (*QQ, QL, QN*) over the control group (*C*). Instead, the results showed a marginally significant difference ($p < .1$) of *C* over *QL*. A cursory explanation for this might be attributed to both the length of the experiment and task saturation. The sessions in this experiment typically lasted for at least 90 minutes, with Simulation 2 taking place about 60-70 minutes into the session. The simulations were fast-paced, with subjects being flooded with information to sort through. The simulations may have been considered a heavy mental workload. Although the treatment was designed to be an aid in detecting discrepancies, it may have merely added to subjects' mental workload,

causing the opposite of the desired outcome. Since the control group received no treatment, subject cognitive load may not have been as heavy.

The unexpected significant difference was between the *QN* and *QL* groups, which was not part of the propositions. Propositions 1-3 compare subjects trained in both quality and quantity dimensions with subjects in a control group, while Propositions 4 and 5 compare subjects trained in both quality and quantity with subjects trained in quality only or quantity only. The results of the Tukey HSD test showed a significant difference of the *QN* group over the *QL* group ($p < .05$). An explanation having to do with the type of deception represented in the simulations is offered. As noted, the simulations were in fast-paced environments. Subjects in the QQ and QN groups were trained that a track received one to three messages, depending upon which radar detected it. They were also told that either no messages or more than three messages may be indicators of deception. With regard to quantity, this meant they were looking for the existence of a message, not necessarily the content itself. In the *QQ* and *QL* groups, subjects were trained that there may be inconsistencies between the information they received from multiple sources. For example, a message from a directly linked radar may contain information about a track that is different than information about that same track received over a network. Detection of this would require more scrutiny of the information by the subject rather than just the existence of a message. Thus, the quantity violations may have been easier to detect.

The significant difference between the means of the *QN* and *QL* groups was interesting. Therefore, two other analysis tests were conducted. Individual one-way ANOVAs between all the groups were run for confirmation of the significant differences

(Table 6). The results confirmed the significant difference between *QN* and *QL*. The significant difference between *C* and *QL* was also confirmed.

Table 6. Summary of Simulation 2 ANOVA Results

Proposition	Analysis	df	Mean Square	F	p
P1	**QQ – C**	1	.013	.779	.394
P2	**QL – C**	1	.103	8.722	.010**
P3	**QN – C**	1	.009	.421	.527
P4	**QQ – QL**	1	.037	3.020	.104
P5	**QQ – QN**	1	.043	1.828	.199
	QN – QL	1	.176	9.957	.007*

**p < .05
* p < .01

A paired-samples *t* test was conducted for a within-groups comparison of improvement from Simulation 1 to Simulation 2 (see Table 7 below). However, these results also indicated no significant differences between Simulation 1 and Simulation 2, suggesting that there was no significant improvement of any one group from the first simulation to the second. Possible explanations for this will be discussed in Chapter 5.

Table 7. Paired-Samples T Tests Between Simulations

Group	Mean Differences (%)	Std. Dev. Differences (%)	t	p
QQ	4.3	14.1	.801	.453
QL	0.0	6.6	-.003	.998
QN	-8.5	13.4	-1.793	.116
C	-7.6	19.2	-1.119	.300
Overall	-3.1	14.2	-1.232	.227

Summary

Overall, no empirical support was found for the propositions, as summarized in Table 8 below. There was a significant difference between the Quality and Control groups in favor of Control, contrary to expectations. An unexpected result, independent of any of the propositions, showed a significant difference between the Quantity and Quality groups.

Table 8. Summary of Proposition Results

Proposition	Description	Supported?
P1	*QQ* will perform better than *C*	No
P2	*QL* will perform better than *C*	No
P3	*QN* will perform better than *C*	No
P4	*QQ* will perform better than *QL*	No
P5	*QQ* will perform better than *QN*	No

Implications of non-support for the propositions will be discussed in Chapter 5. Limitations, conclusions, and recommendations for future research will also be addressed.

V. Discussion

Results

Generally, it was expected that those subjects who were trained in contextual-based methods of deception detection would perform better than those who were not. As shown in Chapter 4, this was not the case, and thus none of the propositions presented in this study was supported. The one-way ANOVA results in one case were the exact opposite of what was expected. The results showed that there was a significant difference between the *QL* and *C* groups, but in favor of *C*. One reason for this result may have been a result of task saturation. A session was typically 90-100 minutes in duration, with Simulation 2 taking place towards the end of the experiment. The treatment for the *QL* group took place just prior to the start of Simulation 2. Although the treatment was designed to enhance deception detection, it actually might have contributed to the mental workload that subjects in the group were experiencing. Since the *C* group received no treatment, then they did not experience an additional mental workload. It is also possible that the subjects receiving the training in quality did not fully understand the characteristics that could indicate deception. Use of the discrepancy button might not have been clear, which is discussed in the limitations portion of this chapter.

An unexpected result, independent of the propositions in this study, showed a significant difference between the *QN* and *QL* groups, in favor of *QN*. It is not clear why this was so, however, some possibilities are likely. Chapter 2 discussed that within

interpersonal communication, successful deceivers typically choose concealment over falsification of information (Ekman, 1985). This suggests that deception involving manipulation of the quality of information is likely to be detected. Applying this concept to the current study, however, the opposite trend is found. It suggests that manipulation of the quantity of information is more likely to be detected. This might be due to the nature of the experimental environment. Subjects received information from multiple sources and were responsible for reporting any discrepancies in the information. Quantity discrepancies were either no messages for a track, or more than three messages for a track. An example of a quality discrepancy was more complex, such as a directly linked radar reporting flight information for a track, but the fused information for the same track received over the computer network being different. An explanation why quantity discrepancy would be detected over a quality discrepancy could be that, given the fast-paced environment, a quantity discrepancy might require less scrutiny than a quality discrepancy.

Limitations

There were several potential limitations to this study. It is questionable whether subjects were truly motivated to participate. Some received extra credit in a class for their participation. Although the informed consent form stated that participation was strictly voluntary, subjects may have felt compelled to participate in order to receive the extra credit. Subjects were told that their names would be entered into a drawing for a gift certificate from Pizza Hut. A better motivator would have been that the subject with

the highest overall score on the simulations would receive the certificate; however, this was not possible, because when simulations unexpectedly terminated early, it was not possible to record the score. Finally, the data collection timeframe took place around mid-term exams, so some subjects were already tired coming into the experiment. Future experimenters are advised, when using a subject population of students, to pay heed to academic schedules to avoid conflicts with breaks, major projects, or exams. It is also recommended to build stronger motivators into the experiment.

The scoring system of the program itself detracted from the purpose of the study. Initially, subjects were told to maximize their overall scores, although the true measurement of the experiment was the percentage of correct discrepancies they reported during the simulations. One scoring component was that a point was deducted every second that a hostile aircraft remained within airspace boundaries. Instead of comparing information from multiple sources to determine if an aircraft was truly a hostile or a friendly, many subjects instead watched the score, determining that aircraft was hostile if points were subtracted from their score. If this particular program is to be used in future experiments, a better scoring system is necessary.

Feedback received during the pilot study indicated that how to use the discrepancy button and its function needed to be clarified in the main experiment. The experimental script was updated accordingly, but possibly to no avail. Although subjects were told that the network was vulnerable to information manipulation and shown how to use the discrepancy button when they detected discrepancies, some did not seem to understand why or neglected to ask if they forgot.. The infrequent to no use of the discrepancy button was slightly exacerbated by the fact that although a reported

discrepancy might be recorded, the system provided no feedback. Some subjects assumed that a lack of feedback indicated the discrepancy button was not working, and indicated that they therefore stopped using it. Others said they were not sure about what the purpose of the button was, but did not bother to obtain clarification. In an effort to avoid giving the true nature of the experiment away, subjects were reminded that the system they were using was a prototype and still under development. The more accurate discrepancies they identified and reported, the higher probability of successful defense from information warfare attacks would be in future versions of the system. Most subjects seemed to be appeased by the answer, when it was still early enough in the simulations for the answer to motivate them to report the discrepancies. In subsequent sessions, subjects were informed that although they would not receive feedback when they reported discrepancies, it was still necessary to report them and that the reports were recorded by the Air Operations Center.

The multiple-choice questionnaires used to determine the effectiveness of the system training and the contextual-based training received during the treatment should be reexamined. Although the instruments seemed to be adequate based on the pre-pilot and pilot studies, questionnaire results from the main experiment suggest otherwise, as summarized in Table 9 below.

Table 9. Training and Manipulation Checks – Main Experiment

DDD Training			
Question	**Number Correct**	**Number Possible**	**Percent Correct (%)**
1	28	32	87.5
2	32	32	100
3	29	32	90.6
4	27	32	84.4
5	20	32	62.5
Contextual-Based Training			
Question	**Number Correct**	**Number Possible**	**Percent Correct (%)**
DDD1	24	24	100
DDD2	24	24	100
Quality1	9	16	56.3
Quality2	9	16	56.3
Quantity1	8	15	53.3
Quantity2	8	15	53.3

The DDD training results show overall that the system training seemed to be effective. This is supported by the results of the generic DDD questions that were on the treatment training questionnaires as well. However, the results for the contextual-based training are drastically different from those from the pilot study. One explanation might be in how the pilot study was conducted. Recalling from Chapter 3 that sessions in the main experiment were homogenous (e.g., all *QQ*, *QL*, *QN*, *C*), all pilot study subjects were in the same session in order to save time. When it was time to apply the treatment, each subject was brought in separately, read to from the appropriate script, and then completed the associated questionnaire. For example, the subject in the *QQ* group was brought in alone, read to from the *QQ* script, and then completed the *QQ* questionnaire. The

individual left, and then the next subject of a different group was brought in. Once the three treatment groups received the manipulation, they were all brought back in and were allowed to begin the second simulation. The fact that the treatment subjects received the manipulation one-on-one with the experimenter, they might have focused more on the training since there were no others in the room. In the main experiment, most sessions had three to four people at one time. However, this explanation is admittedly inconclusive, since there was only one subject per group. Another reason why subjects may not have received better questionnaire scores was that questionnaire results were determined after data collection was complete. A better approach might have been looking at the answers while the subjects were present, going over any incorrect answers for clarification, and then allowing subjects to start the simulations.

The computer program itself would benefit from better design. One unexpected problem was that some subjects reported difficulty distinguishing between red and green colors due to colorblindness. Designing the system with other colors would compensate for this. Subjects also recommended different design features be implemented. For example, some thought it would be useful if the program automatically grouped messages received by track numbers rather than times so that they did not have to scroll back through the messages sequentially.

The most frustrating issue was the apparent instability of the computer systems. For reasons undetermined, the programs sometimes terminated in the middle of a simulation. One possible reason is that subjects may have accidentally clicked both the left and right mouse buttons at the same time. It was suggested that this might cause the program to terminate because clicking both buttons has a specific function in the Linux

operating system. It is unknown if the unexpected termination of programs was program-specific or Linux platform-specific. After a few instances of self-terminating programs, the X-window servers were restarted between simulations, and the computers themselves were rebooted completely between sessions to help stave off the undesired glitch. The combination of the actions seemed to help somewhat in that there were less unexpected program terminations during the remainder of the experiment. Subjects were also asked to be mindful of not clicking both mouse buttons simultaneously, in case that was the reason for unexpected termination. When this problem occurred, subjects were given the choice of restarting the simulation or merely ending their participation with no penalty. Following the precedent set in the Fields (2001) and Langhals (2001) studies, data from simulations were considered usable if subjects were able to play for at least fifteen minutes into a simulation. Fortunately, the true measures of performance were based on percentages of accurate discrepancies identified, and not the overall simulation scores because most scores were not available when a simulation terminated unexpectedly. There was only one subject who opted to cease participation rather than restart the simulation.

The initial system training at the beginning of sessions was most likely insufficient, particularly the hands-on portion. The hands-on portions lasted about ten minutes, which included a walk through of the tasks and using the remaining time as practice. Subjects had different learning curves and some grasped the concepts and associated concepts more quickly than others. In addition, there were times when subjects would try to perform tasks ahead of the other subjects and not hear how to perform the current task. This caused the experimenter to have to repeat how to perform

tasks. The inattention of one subject might have caused the other subjects present to miss something because of the interruptions. Subjects were asked in subsequent sessions to please stay with the group so no one would miss instructions. Insufficient training time more than likely worsened any task saturation that subjects experienced. Given the fast-paced environment, Simulation 1 may have inadvertently served as an additional practice round. By the start of Simulation 2, most subjects were probably mentally fatigued from task saturation, thus causing the treatment to have no effect on their performance.

Methodology itself is always an issue to look at when discussing limitations of a study in which the hypotheses, in this instance, propositions, are not supported. This study is no different. Laboratory settings are usually limitations because it is rarely possible to have a truly realistic environment. The simulations were individual subject efforts, although they were in a group. Performance might improve by segregating subjects with partitions, or run individual subject experimental sessions. Subjects were responsible for watching three radars simultaneously; whereas in a real-life situation, they would probably only focus on one. In a real-life setting, there is no point system. Success is measured by maximum damage to the enemy, with zero loss of life and minimal damage of assets to friendly forces. Finally, the total number of subjects among all the groups was thirty-two; the results could have been significantly different had a much larger sample size been used.

Implications for the Air Force

The results of this study are not necessarily disheartening. The study was conducted under an exploratory umbrella. This was because little research has been done regarding artifact-based deception detection. This study attempted to adapt principles from interpersonal trust and deception detection and apply them to human-artifact deception detection. The bottom line for the Air Fore is merely that the arena of artifact-based deception detection is wide open for further study.

It is not entirely surprising that the propositions of this study were not supported. Research in interpersonal deception detection training, as discussed in Chapter 2, is inconsistent. Generally, deception detection is low in human-human interactions. Some researchers have found that training has little effect on detection accuracy (Vrij, 1996, Feeley and deTurck, 1997). However, some researchers found that moderate suspicion may enhance it (McCornack and Levine, 1990). In human-artifact interactions, individuals tend to trust automation to the point of committing errors of commission and omission. Another study found that training information systems users had no significance on accurate detection (Biros, 1998). However, another study suggests that using incentive structures can facilitate data error detection (Klein and Goodhue, 1997). Therefore, the inconclusive results of this study are in line with the inconsistency of existing research.

Proposed Future Experiment

A proposed experiment using the Dynamic Distributed Decision-Support System (DDD) is offered to account for the limitations of the current study. The general pretest-posttest design should still be used. Taken together, implementing the items discussed below should provide a more sound experimental methodology.

First, the DDD system design should be improved to correct its instability. This will ensure that the simulations run for the required time and allow a better scoring system to be implemented. The color scheme should also be altered to avoid the potential issues associated with colorblindness of subjects.

Motivation in the current study seemed to be lacking. Therefore, it is important to provide stronger motivation for subjects in the future experiment. Assuming the instability of the current DDD system design can be remedied, then a different scoring system that potentially appeals to individuals' competitive sides can be implemented. Subjects were told in the current study that their performance would be measured by their combined offensive and defensive scores in order to motivate them to perform well. This was not actually the case, but the purpose of the study required them to be told this. It was not possible to use the combined scores fairly because scores were not available when some programs terminated. With the instability fixed, this scoring system could be actually be implemented. However, it would be more useful to hide the score from subjects during the simulation, since theoretically not seeing a score until after the simulation should motivate them to do as well as they can. Hiding the scores during simulations would also keep subjects from watching score deduction to determine if a

track was truly hostile. Finally, if subjects are to be taken from a pool of students, it is recommended that data collection not coincide with major projects, exams, or holidays.

The true performance measure of this study was the percentage of accurate discrepancies reported. An issue with the current study seemed to be that the use of the discrepancy button was not necessarily clear. The future experiment should strive to make use of the discrepancy button clearer. Several subjects stated that they stopped using the discrepancy button because they received no feedback from the Air Operations Center when they reported discrepancies. This observation is in line with Zuckerman et al's (1984) interpersonal deception study that said peoples' deception detection abilities seem to increase with feedback. In their study, subjects judged the truthfulness of confederates' messages. Afterward, the judges were told how accurate they were as well as what clues they had missed on the inaccurate judgments. Based on the feedback, subjects learned from their mistakes and improved their abilities. Designing a feedback mechanism into the DDD system should encourage subjects to use the discrepancy button as they are instructed and possible provide more accurate results.

Increased care should be taken to validate instruments in future experiment. It is recommended that more pilot study subjects be used to achieve this. In addition, answers to the manipulation checks should be discussed with the subjects during the experiment sessions, but prior to participation in the simulations, to give the experimenter the opportunity to clarify any misunderstandings with system training or treatment training.

Subjects in the future experiment should have longer training periods, since the length of training in the current study appeared insufficient. Enough training time should be given to subjects so that they may be considered experienced operators when it comes

time for the actual simulations. Biros (1998) found that individuals who were experienced in the information system used in his study performed better than novices. Ideally, multiple practice sessions would help as well to avoid short-term memory loss.

As discussed earlier, task saturation seemed to be a problem with the current study. The future experiment should take steps to mitigate this effect. Reducing the number of tracks appearing in the simulations may help to do this. Tracks appeared in waves throughout the current simulations. Reducing the number of tracks appearing during a wave may also help, since this would reduce the number of associated messages that subjects have to analyze as well. Laboratory environments are often criticized because they typically do not accurately reflect the environments in under study. Feedback from subjects suggested that responsibilities for only one radar would be more realistic. The current study had subjects responsible for three radars. Cutting back to one radar would likely help to reduce task saturation.

Finally, it is recommended that the future experiment draw from a subject population of individuals who might actually use systems similar to the DDD system. Such a population could consist of AWACS operators or United States Army Air Defense Artillery personnel. This might motivate subjects to perform well since the type of system used is relevant to their daily jobs.

Other Recommendations for Future Research

This study used Information Manipulation Theory (McCornack, 1986) as the basis for the experiment used. Although the propositions for the study were not

supported, contextual-based methods for detecting deception should not be ruled out. The current study only tested the maxims of quality and quantity of IMT because the computer program used made it possible to gather this empirical data. The significance difference between the *QN* and *QL* groups might warrant a separate study comparing quantity violations versus quality violations. Finally, studies might benefit from exploring the maxims of relation and manner as well.

Klein and Goodhue (1997) suggested that incentive structures paired with goals in error detection is possible. They also mention theories of individual task performance that "provide some guidance for identifying conditions under which users can improve their discriminability" (Klein and Goodhue, 1997:1-29). A study conducted by Biros (1998) supports that of Klein and Goodhue. He found that experience within an information domain influenced artifact-based deception detection ability, while training alone seemed to have no effect.

Another recommendation for future research is to use an information system that is common to more users, preferably in an environment that is close to the one in which the system is normally used. This would be difficult, however, since natural environments and experiments are typically mutually exclusive. The information system used in this environment of this study was unfamiliar to the users; they were expected to receive a short training program and then perform accordingly. The fast pace of the environment created for this study was more than likely not one common to most users. It would be useful to look at certain information systems indigenous to specific career fields. This way, the learning curve to operate the system may be smaller.

The limitations and above recommendations discussed suggest that artifact-based deception detection training may be dependent upon particular information domains. A work environment can be considered an information domain. To thrive in the domain, an individual must gain experience. The information systems found in that particular domain may not be one that is found in a different environment or domain. Logically, training such an individual to detect deception in the information the system provides would have to be specific to that system. It is not likely to create an artifact-based deception detection training program that would encompass all information systems. Information systems are designed for specific purposes to be used in specific environments, or rather, information domains. This suggests that since most information systems are different, then the ways that deception can occur will also differ. Therefore, training in their use would also have to be different, and hence, deception detection training would have to be particular to a system. Since the Air Force uses information systems in all day-to-day and mission operations, this approach might prove the most logical, useful, and worthy of pursuing.

Conclusion

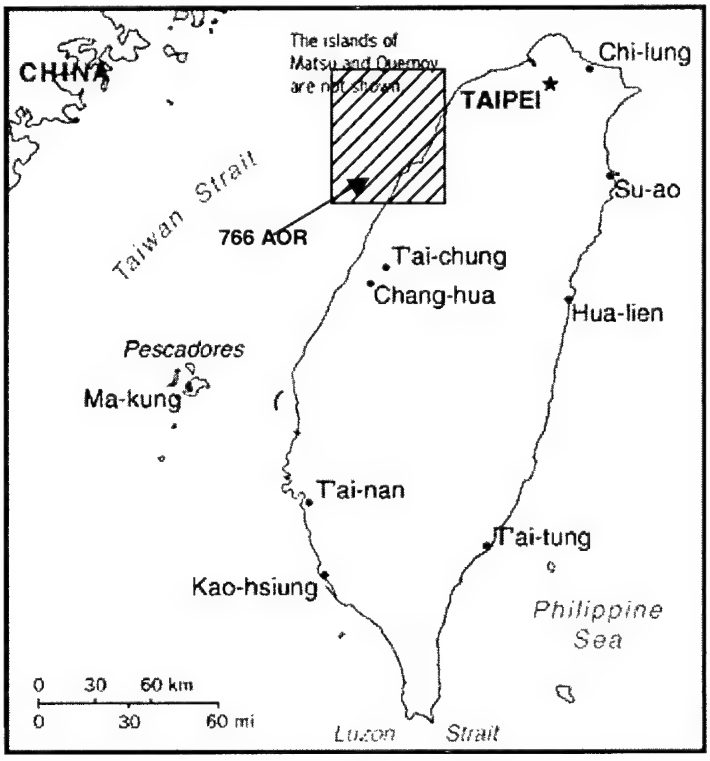
The literature review and results of this study have several implications for the Air Force. There is still much to be learned about human detection of artifact-based deception. The heterogeneity of information artifacts throughout the Air Force will likely prove it difficult to develop an overarching program that successfully train users in artifact-based deception. In addition, previous studies suggest that experience, rather

than training, has more of an impact on user deception detection. Experience implies understanding of a user's information domain. These elements taken together suggest that the Air Force will benefit from studying the users and the information artifacts within particular information domains. Developing specialized training programs for specific information domains may help information artifact users increase their deception detection abilities. This, in turn, may serve to ensure the Air Force maintains Information Superiority and Information Assurance.

Appendix A: Scenario Brief

BACKGROUND:

You are the air defense commander for 766th Air Defense Unit deployed in Northwest Taiwan. The 766th is a joint air defense unit that integrates tactical ground radar units and surface-to-air missile defense units into a single weapon system. The ADU is a deployed arm of the Air Operation Center and has data connectivity with the AOC, remote radar sites, and remote SAM sites.



THE PRESENT: You have just received the crew changeover briefing where you received the standard mission briefing, Intelligence briefing, and the Rules of Engagement briefing. The following is a summary of the information you received:

MISSION: Defend the assigned air space against any suspected hostile aircraft. The 766th is one of several air defense units dispersed along the coast of Taiwan. You are responsible for air surveillance, track identification, and weapon interdiction. The commander of the 766th is also responsible for assigning a confidence level to all track information and forwarding that information to the Air Operation Center.

INTEL BRIEF:

In early July, the Chinese government declared it does not recognize the independence of Taiwan, as declared by the Taiwanese government this past June.

In response to this declaration, Taiwan requested and received military support from the United States. This support consisted of two naval battle groups, the regional deployment of 120 fighter and support aircraft, and the local deployment of 5 new Air Defense Units with remotely operated radar and SAM sites.

The deployment was completed in late August. Following this deployment, China threatened that if allied forces were not withdrawn by the first of September then China would reserve the option for a military response. Intel sources and satellite imagery indicate a massive Chinese air assault is imminent.

Intel also reports that the Peoples Republic of China's Information Warfare Force (IWF) have been probing the U.S. forces Wide Area Network. The IWF technology is thought to include some of the most advanced network attack and information manipulation systems in the world. The Chinese have recently demonstrated a successful

Information Warfare attack, known as Strategic Information Manipulation (SIM), against the Taiwanese government. SIM is a technique whereby the network is covertly accessed and real-time tactical or strategic information is manipulated in order to confuse or spoof the enemy

RULES OF ENGAGEMENT: By the order of the President of the United States, all US military forces are authorized to use deadly force to interdict hostile aircraft from entering Taiwanese airspace.

Scenario taken from Fields (2001).

Appendix B: Dynamic Distributed Decision-Support System Training Script

INTRO

Good _____, my name is Captain Elizabeth Autrey. I'm from the Air Force Institute of Technology, AFIT. Today you will be taking part in a study that will be used to examine some human factors issues related to automated decision-support-systems. The particular decision support system you will be using is designed for battle commanders in a distributed deployed environment. For this battle simulation, you will be playing the role of a battle commander in charge of a deployed Air Defense Unit. Your unit is responsible for performing a command and control task while deployed in a high-risk, combat environment. Before we get to the scenario brief, it's necessary for you to become familiar with the DDD system. We'll get started now.

I will give you a short overview of the decision support system, provide instructions on its use and operation. Following this training I'll have you go through two 20-minute simulations. I hope to get you out of here in roughly an hour and a half. If you have any questions at any point during the training, please feel free to interrupt and ask the question.

SYSTEM DESCRIPTION

I will begin the training by explaining the various components of the ADU, the decision support system, and the tasks I will be asking you to perform. Next, I'll put you in front of one of the DDD computers and provide you hands-on training with the system.

Following the hands-on portion, I'll give you a chance to practice what you've learned in a short 10 minute training simulation.

[SLIDE 2] First you need to understand how the ADU is configured. The ADU consists of three main parts: The DDD computer, the sensor sites, and the network.

The DDD computer is capable of establishing up to 100 data links with remote sensor sites. Data links are electronic pathways that use an established protocol for sending and receiving messages. These data link connections are established over a Wide Area Network, or WAN. The DDD computer processes, fuses, and displays all incoming data link messages from sensor sites into a combined graphical display. It also allows the ADU commander to send and receive email messages. Finally, it will give the ADU commander the capability to remotely control one or more weapon systems.

The DDD system is designed to assist the ADU commander by automatically identifying incoming air tracks. It does this by comparing and fusing the information received from the connected sensor sites.

The next part is the sensor sites. The sensor sites send unencrypted air track information to the DDD computer located in ADU battle cab. You will be able to see the messages sent by the sensor sites on the DDD display screen.

The last part of the system is the WAN. The WAN is a standard Air Force wide-area-network that incorporates the latest firewall protection schemes.

These three main components, the DDD computer system, the sensor sites, and the WAN make up the ADU system concept. Are there any questions before I continue?

NETWORK PARTICIPANTS [SLIDE 3]

Besides the sensor sites I've already mentioned, you will also be connected to the Air Operation Center (AOC) and computer emergency response team called the Network Security Force. Communication with these participants will be accomplished through an email system.

The AOC is a simulated participant. They automatically receive information from all the ADUs in the AOR. The AOC monitors battle activity and will alert you of possible dangers or mistakes.

The Network Security Force (or NSF) is the other participant. The NSF is a specialized computer emergency response team (CERT) that specializes in Defensive Information Warfare tactics. Their mission is to monitor and protect all networks within an AOR against enemy attacks. These attacks take many forms. For instance, delay of service, network crashing, or information manipulation.

Are there any questions before I continue?

TASK DESRIPTION [SLIDE 4]

For this game, you will have four basic tasks to perform.

First, you must monitor your assigned airspace. You will be able to do this by simply looking at the graphical battle space display and monitoring any tracks that look like they may attempt to enter your protected air space.

Next, you must determine the identity of an air track about to enter protected air space. You can do this by using the information provided on the graphical display system, reading the individual messages from the sensor sites, or both. If you detect a

discrepancy between the information on the graphical display and the sensor messages, you will need to send a data alert message to the AOC.

The third task is the assignment of a confidence level to a track. The confidence level is a number between 1 and 5 with five having the highest confidence and 1 having the lowest. Once set, this information is automatically broadcast to the AOC who will use this information to generate alerts and allocate resources.

The fourth task is your decision to either allow a track to enter into protected air space or attack the track with a SAM before it enters the air space. You'll learn how to perform all the mechanical functions for these tasks in a few minutes. Are there any questions?

DISPLAY DESCRIPTION [SLIDE 5]

Now that we've looked at the ADU system, I'm going to describe the various parts of graphical display for the DDD computer. This is a screen shot of the DDD computer system display. The display consists of five main regions.

[SLIDE 6] The first region is the battle space display. Track icons, track information, airspace boundaries, and sensor ranges are displayed in this region. I will show you how to interact with the icons in this region during the hands-on portion of training.

[SLIDE 7] The next region is the Scoring/Display Control window. This region displays your offensive and defensive scores. It also displays various buttons that allow you to control display settings, such as zooming in and out, as well as a slider type scale that will show you the time to completion for certain tasks.

[SLIDE 8] The next region is the e-mail region. This is where you can view track information messages sent by the sensor sites. You will also receive e-mails from the NSF here. As you will see during the practice session, the NSF can set the priority such that the email will automatically open up for viewing. Note here in the email messages that the radar that sent the message is colored; it corresponds to the color of the radar on your display screen.

[SLIDE 9] The next region is the report window. This will automatically display the titles of incoming emails and other messages sent to the system.

[SLIDE 10] Finally, the last region is the System message window. This window will display automated system messages that give information about your assets, your actions taken, and threat information.

Are there any questions on any of the regions?

ICON DESCRIPTION [SLIDE 11]

Now I'm going to quickly go over the icons you will be working with. The first is a Hostile track represented by an upside down "V" and colored red. All tracks have a red vector line that indicates direction (in which the vector line is pointing) and speed. The upside down green "U" is a friendly track. The colored squares represent friendly assets. You will be red; so all the systems colored red will be under your direct control.

Any questions on the icons?

[SLIDE 12] This next slide shows another display function, the sensor rings. The dark blue rings are the detection zones for each radar. Tracks entering this zone will be detected and identified by sensors, and a message will be sent to your display. 1-3 messages will be generated for each track, depending upon which detection zones they

enter; a radar will only generate 1 message per track it identifies. Information on the altitude, speed, and heading of each track will be included in the messages. A red ring indicates a weapons range. For you, this will be the range of the SAMs under your control. You will only be able to attack tracks once they have entered the red zone. Finally, the yellow zone indicates the vulnerability zone for each asset. Enemy tracks that penetrate this zone will be able to destroy that asset. In additions, if enemy tracks get too close within these zones, you may not be able to destroy them. Any questions?

As I mentioned early, one of the participants for this game is the NSF who will be monitoring and defending the network against attacks. The computer will simulate the NSF. In addition, the computer may simulate random information warfare attacks. The likelihood of a successful attack will not be disclosed. However, you may be notified via email if an attack is detected.

SCORE SYSTEM [SLIDE 13]

Finally, let's go over the scoring system I will use to evaluate your performance. In essence, this game is a strategy game. For your part, I want to you to focus on maximizing your score. In a real life situation, a maximized score means zero friendly aircraft lost and maximum damage to the enemy. For this game, however, a maximized score means the highest possible offense and defensive score combinations. The scoring system reflects real-life risks and pay-offs associated with strategy choice.

The scoring system is based on your ability to correctly identify a track and the confidence level you place in your identification decision. Your offensive and defensive score is calculated using the scoring table provided at your station. The more confident you are in your identification decision the greater the payoff to your offensive score when

you shoot down a hostile aircraft. However, big payoffs are often tied to big risks. Therefore, the more confidence you place in your identification decision, the greater the loss to your defensive score if you shoot down a friendly aircraft. Finally, because your mission is to prevent hostile aircraft from entering your airspace you will lose one point per second from your defensive score for the duration the hostile remains in your airspace.

All participants' names will be entered into a random drawing for a $25 gift certificate for Pizza Hut.

Any questions?

HANDS ON PRACTICE [SLIDE 14]

Now let's go over to a computer and get familiar with the different functions. The first thing I'll ask you to do is to click the Start button. This will start the simulation. Go ahead and left click it now. The clock in the upper right portion of the screen should have started counting.

Task	Action
Get information on asset	Right click on asset and select Info on Asset (Note: you must hold the button down as you select). On the SAM sites, "Attack" is the only functional option out of the list.
Assign Confidence Level	Right click on track and select Identify. Slide the button on the confidence level bar. 5 denotes the highest confidence, while 1 denotes lowest. The level you assign will appear on the screen in parentheses after the track number. You can change the confidence level at any time. You must assign a level other than 0 before you can attack. Press OK when finished.

Attack Track	Right click on SAM site and select attack. Note: track must be inside red circle. The icon becomes a cross-hair. Place the cross-hair on the track and Left click. The icons turn to squares with X's in the middle; this indicates they are busy engaging. While engaged, a SAM cannot be used to shoot another track until finished.
Open email.	Double Left click on the email subject in the email window. When finished reading, click either Close or Delete.
Zoom In-Out	Click on the Zoom in button and either Left click on any spot on the battle space window, or Left click and hold the button down while dragging the icon. A green square will appear. When you let go of the button the screen will zoom into the region. To Zoom out, simply Left click on the Zoom Out Button. However many times you zoom in is how many you must zoom out to return to the normal display.
Cancel	Left click on the Cancel button to cancel a function before you have taken the action.
Discrepancy Button	You need to push this button located on Task Identify window if you notice a discrepancy between what is displayed on the graphical battle space display and the individual messages from the sensor sites. This is actually an important feature. As mentioned, this system is a prototype, with one objective as being able to defend against IW attacks. The more legitimate discrepancies that are reported, the higher the probability of successful defense from IW attacks in future versions of the system.

Now go ahead and play for a few minutes on your own. Practice using your SAMs to attack, assigning confidence levels, and transferring information to the ROC. Pay attention to the system message and report windows. [Also, look for a sample message from the Network Security Forces.] Let me know if you have any problems.

QUESTIONAIRE [SLIDE 15]

Before we take a break and go on to the final simulation, I need each of you to complete another short survey. This information will help determine, among other things, how effective training on the DDD was. This information will be kept confidential and your names will not be associated with the survey following the experiment. Once you're done, please take a short 5-minute break.

BREAK

FIRST SIMULATION [SLIDE 16]

Please take your places in front of the computer, but do not click on the Start button until you are instructed. OK, please read the simulation scenario to yourselves as I read it out loud. *[When all are done, ask]* Are there any questions on the scenario? Are there any other last minute questions? When you are done with the simulation, please stay at your computer stations until told otherwise. OK, click on the Start button and begin.

SHORT BREAK

TREATMENT

TREATMENT SURVEY

SECOND SIMULATION

DEBRIEFING

Adapted from Fields (2001) and Langhals (2001).

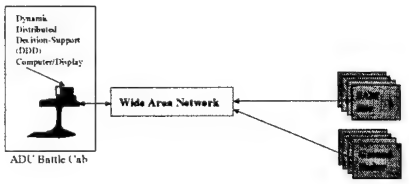
Appendix C: Dynamic Distributed Decision-Support System Training Slides

Air Defense Unit (ADU)

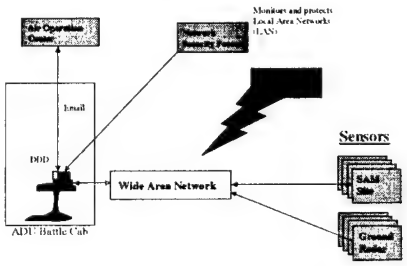
Dynamic Distributed Decision-Support (DDD) System

Field Evaluation

ADU System Description

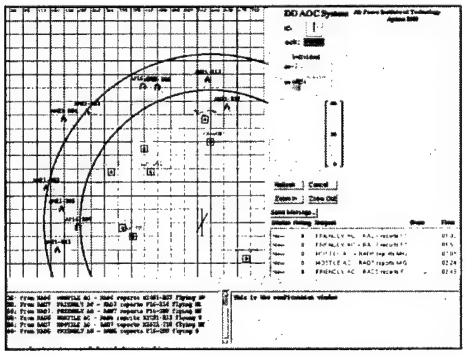


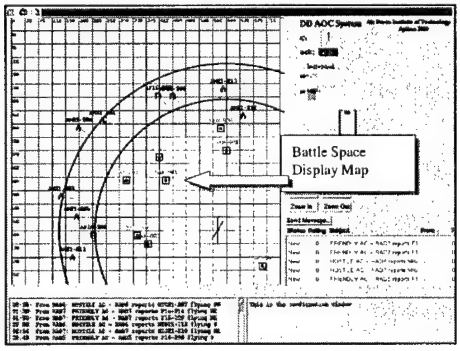
Other Network Participants

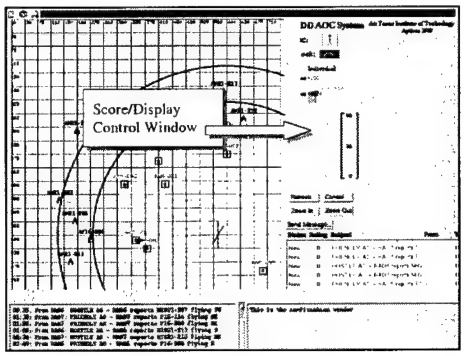


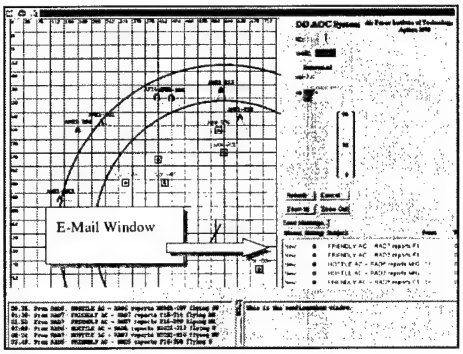
ADU Commander Tasks

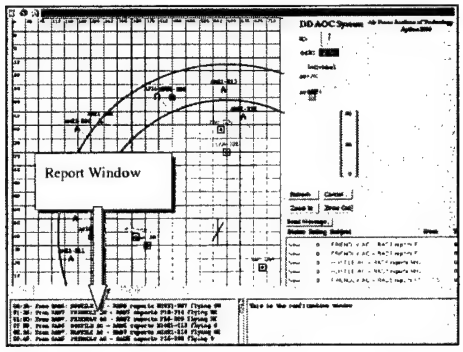
- Monitor Air Space
- Determine Identity of Air Tracks
  - DDD Graphical Display
  - Raw Messages from Sensor Sites
- Assign a Confidence Level to the Track
- Either allow access to protected air space or attack using a Surface to Air Missile

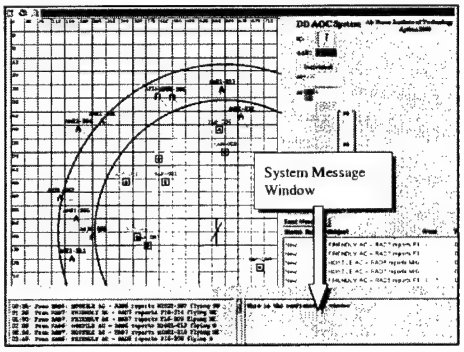


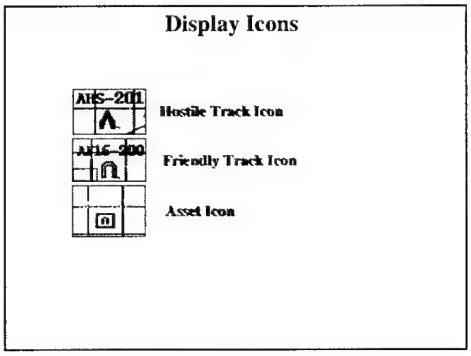


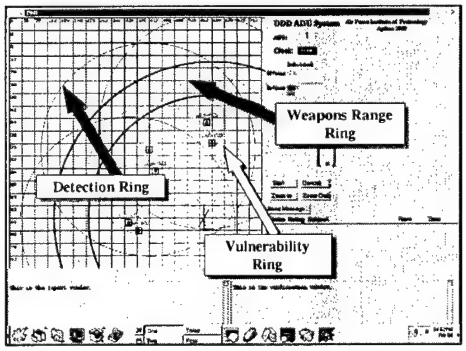


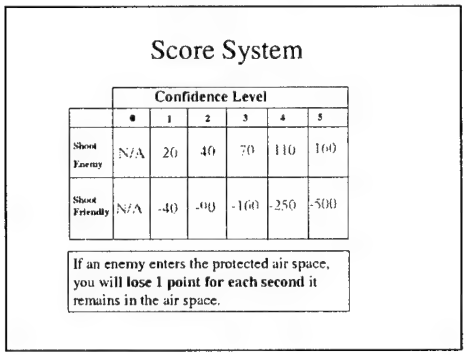












All slides taken from Fields (2001).

Appendix D: Subject Demographics

Table 10. Subject Demographics

Subjects per Treatment			Subject Rank (Military)		
Treatment	# Subjects	% Total	Rank	# Subjects	% Total
QQ	7	21.9%	2d Lt	1	3.3%
QL	9	28.1%	1st Lt	13	43.3%
QN	8	25.0%	Capt	14	46.7%
C	8	25.0%	Maj	1	3.3%
Total	32	100%	Lt Col	1	3.3%
Ops. Experience (Combat/Hostile Duty)			Highest Education Level		
Ops Experience	# Subjects	% Total	Education Level	# Subjects	% Total
Yes	10	31.2%	Bachelors Degree	28	87.5%
No	22	68.8%	Masters Degree	4	12.5%
Subject Years in AFSC			Subject Total Years in Service		
Years AFSC	# Subjects	% Total	Total Yrs Svc.	# Subjects	% Total
0-5	20	62.5%	0-5	11	34.4%
6-10	8	25%	6-10	5	15.6%
11-15	1	3.1%	11-15	10	31.2%
16-20	2	6.3%	16-20	4	12.5%
Over 20	1	3.1%	Over 20	2	6.3%
Subject Branch of Service			Subject Age		
Branch of Service	# Subjects	% Total	Age	# Subjects	% Total
USAF	28	87.5%	20-25	4	12.5%
Civilian	2	6.3%	26-30	12	37.5%
Foreign	2	6.3%	31-35	10	31.2%
			36-40	4	12.5%
			Over 40	2	6.3%

Appendix E: Demographics and Computer Beliefs Questionnaire

Participant Information Sheet **Participant # _____**

INSTRUCTIONS

This is a short two-part survey to determine the demographic information of the participants in this research as well as their experience level with computer systems. The data collected will be used to aid in the evaluation of the results of the simulation. All information provided will be kept confidential and will not be able to be traced back to the participant.

SECTION 1 – Demographic Information

1. Age _____

2. Rank _____ Service (USAF, Army, Navy) _____

3. AFSC _____

4. Number of years served in current AFSC _____

5. Total number of years served in the military _____

6. Highest Level of Education (circle one): High School, Undergraduate, Graduate, Doctoral

7. Operational experience in Combat/Hostile Duty Location (yes/no) _____

SECTION II: Computer Beliefs

Please answer all of the questions below. Use the scale provided and enter the number that best matches your beliefs.

1 = Strongly Disagree; 2 = Disagree; 3 = Somewhat Disagree; 4 = No opinion

5 = Somewhat Agree; 6 = Agree; 7 = Strongly Agree

1. _____ If you initiate a task for the average computer system to perform, the computer system will finish it correctly.

2. _____ I believe that most computer systems are consistent.

3. _____ Most computer systems are reliable.

4. _____ I believe that most computer systems are technically competent.

5. _____ I feel I can depend on most computer systems.

6. _____ I can trust most computer systems.

Demographics and questionnaire taken from Fields (2001).

Appendix F: Dynamic Distributed Decision-Support System Training Questionnaire

Training Evaluation 1 **Participant #:_____**

INSTRUCTIONS

The information you provide will be kept confidential. In addition, your identity will not be linked to this data. The information collected from this form will be used to help evaluate the ADU computer system and training program.

Please circle the correct answer:

1. The role of the Network Security Force is to _____
   a. Monitor the network only
   b. Protect the network only
   c. Monitor and Protect the network
   d. None of the above

2. An upside "V" shaped icon that is colored red represents what type of track? _____
   a. Friendly
   b. Hostile
   c. Unknown
   d. None of the above

3. Which of the following are Information Warfare tactics? _____
   a. Denial of Service
   b. Information Manipulation
   c. Hacking
   d. All of the above

4. The main components of the ADU are _____
   a. The DDD computer system, the WAN, and the sensor sites
   b. The DDD computer system and the Network Security Forces
   c. The Network Security Forces, the DDD computer system, and the WAN
   d. None of the above

5. Track identity is automatically determined by DDD. A secondary means by which you can verify the track identity is to _____
   a. Send a request to the AOC
   b. Read incoming messages from the sensor sites.
   c. None of the above
   d. All of the above

Training questionnaire taken from Fields (2001).

Appendix G: Quality-Quantity Training Questionnaire

Training Evaluation 2a **Participant #:_____**

INSTRUCTIONS

The information you provide will be kept confidential. In addition, your identity will not be linked to this data. The information collected from this form will be used to help evaluate the ADU computer system and training program.

Please circle the best answer:

1. Knowing how information can be manipulated can help assess message _____
   e. Length
   f. Sources
   g. Validity
   h. None of the above

2. Either too much information or too little information within a message is an example of a _____ violation.
   e. Reliability
   f. Quantity
   g. Content
   h. None of the above

3. When an adversary has manipulated information to make a hostile aircraft appear as a friendly aircraft, this is an example of a _____ violation.

   a. Network
   b. Quality
   c. Context
   d. None of the above

4. Deceptive messages are produced by _____ manipulating information.

   e. Covertly
   f. Intentionally
   g. Both a and b
   h. None of the above

5. False information intentionally inserted into a message in order to appear true affects the _____of a message.

   e. Quality
   f. Quantity
   g. Soundness
   h. None of the above

6. In the DDD system information domain, a track appears on the display, but none of the radars provide identification messages. This is an example of a _____.

   e. Malfunction
   f. Quality violation
   g. Quantity violation
   h. None of the above

Appendix H: Informed Consent Form

Study Overview

Welcome to the experiment. The following is a general description of the study and a reminder of your rights as a potential subject. As in any study, your participation is completely voluntary. If now, or at any point during the study, you decide that you do not want to continue participating, please let the experimenter know and you will be dismissed without penalty. Also, please remember that your name will not be associated with any of the information that you provide during the study. All of the information you provide is absolutely anonymous and confidential.

In this study, you will be working individually to complete a mission objective. You will also be asked to complete some questionnaires during the study. You will first be given a questionnaire to complete, and then following the training, you will be given other questionnaires to complete. The experimenter will give you more specific instructions later in the study. If you have any questions or concerns at this time, please inform the experimenter.

For further information

The Air Force Institute of Technology faculty member responsible for conducting this research is Maj. David Biros. He would be happy to address any of your questions or concerns regarding this study. Maj. Biros can be reached at 255-3636 ext 4578.

If you would like to participate in this study, please sign in the space provided. Your signature indicates that you are aware of each of the following: 1) the general procedure to be used in this study, 2) your right to discontinue participation at any time, and 3) you and your name will not be associated with any of the information you provide.

Printed Name: _____

Signature: _____ Date:_____

Informed consent form adapted from Fields (2001).

Appendix I: Quality-Quantity Treatment Script

As you have just seen from your first round, the Dynamic Distributed Decision-Support (DDD) System provides vast amounts of information at a relentless rate that you, as the decision maker, must sort through and use to make time-critical decisions. It is imperative that you have the right information, the right amount of information, at the right time. Ensuring you have the right information when it is needed is even more difficult in an Information Warfare environment, due to the potential of network and information attacks. Network security can be compromised, allowing adversaries to gain access to information, directly alter information, or perform other network attacks.

Think back a few minutes ago to your experience with the DDD. Are you certain you had the right information? Were you lacking information? Are you certain that the information that this system presented you to aid in your decision-making was factual, and not altered by an adversary? How do you hone in on the right information, and will you be able to detect deceptive information?

Research suggests that information systems users can be taught to better recognize deception. An integral part of detecting deception is understanding the information domain of which you are part; for instance, knowing your sources of information – where it comes from, how information is used, and how it moves through your domain. Due to the nature of your profession, these domains will change, as will the knowledge you will need to understand them.

Research indicates that messages are received with the expectations that they are sound within the dimensions of Quantity and Quality. Deceptive messages are produced by covertly and intentionally manipulating information along one or both of these dimensions. Knowing the nature of the dimensions can assist in assessment of message validity. Violations along these dimensions may indicate deception. A description of the dimensions follows:

Quantity. This is the amount of information present in a message. Is there enough information in the message to make a positive contribution? Too much information may function as a distracter.

Recall from the initial DDD training that you can receive 1-3 messages per track. Here is a good example of understanding your information domain. When a particular radar detects a track, it will only send one message on that track. Zero messages or more than three messages for a track is a violation of how information appears in your domain, and may indicate an information warfare attack.

Quality. It is expected that information within messages will be valid. False information, appearing to be true, can be inserted into messages.

Discrepancies between information appearing in the report window and the information available on a track can exist.

Keep this in mind for the final round. Are there any questions on the dimensions before we begin?

Bibliography

Anonymous. Maximum Security, 2nd Edition. Indianapolis IN: Sams Publishing, 1998.

Barber, Bernard. The Logic and Limits of Trust. New Brunswick, NJ: Rutgers University Press, 1983.

Bavelas, Janet B., Alex Black, Nicole Chovil, and Jennifer Mullett. Equivocal Communication. Newbury NY: Sage Publications, 1990.

Biros, David. The Effects of Truth Bias on Artifact-User Relationships: An Investigation of Factors for Improving Deception Detection in Artifact Produced Information. Dissertation. Florida State University at Tallahassee, 1998.

Buller, David B, and Judee K. Burgoon. "Interpersonal Deception Theory," Communication Theory, 6(3): 203-242 (August 1996).

Burgoon, Judee K., David B. Buller, Amy S. Ebesu, and Patricia Rockwell. "Interpersonal Deception: V. Accuracy in Deception Detection," Communication Monographs,51: 303-325 (December 1994).

Burgoon, Judee K., David B. Buller, Laura K. Guerrero, Walid A. Afifi, and Clyde M. Feldman, C.A. "Interpersonal Deception: XII. Information Management Dimensions Underlying Deceptive and Truthful Messages," Communication Monographs, 63: 50-69 (March1996).

Denning, Dorothy E. Information Warfare and Security. Reading MA: Addison-Wesley, 1999.

Department of the Air Force. Information Operations. Air Force Doctrine Document 2-5. Washington DC: HQ AFDC/DC, 5 August 1998.

Department of Defense. Joint Doctrine for Information Operations. Joint Publication 3-13. Washington DC: GPO, 9 October 1998.

Department of Defense. Joint Vision 2020. Washington DC: GPO, June 2000.

deTurck, Mark. "Training Observers to Detect Spontaneous Deception: Effects of Gender." Communication Reports 4(2): 81-90 (Summer 1991).

Dooley, David. Social Research Methods, Third Edition. Upper Saddle River NJ: Prentice Hall, 1995.

Ekman, Paul. Telling Lies. New York NY: W.W. Norton & Company, 1985.

Feeley, Thomas H. and Mark A. deTurck. "Global Cue Usage in Behavioral Lie Detection," Communication Quarterly, 43(4): 420-430 (Fall1995).

Fields, Greg. The Affect of External Safeguards on Human-Information System Trust in an Information Warfare Environment. MS thesis, AFIT/GIR/ENV/01M-07. School of Engineering and Management, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, February 2001.

Fogleman, Ronald R., General USAF. "Cornerstones of Information Warfare." Air Force Pamphlet, 1995.

Forrest, James A. and Robert S. Feldman. "Detecting Deception and Judge's involvement: Lower Task Involvement Leads to Better Lie Detection," Personality & Social Psychology Bulletin, 26(1): 1-14 (January 2000).

Grice, H. Paul. "Logic and Conversation," in Syntax and Semantics: Speech Acts. Eds. P. Cole and J.L. Morgan. Academic Press, 1975.

Klein, Barbara D. and Dale L. Goodhue. "Can Humans Detect Errors in Data? Impact of Base Rates, Incentives, and Goals," MIS Quarterly 21(2): 1-29 (June 1997).

Langhals, Brent. The Affect Of Varying Arousal Methods Upon Vigilance And Error Detection In An Automated Command And Control Environment. MS thesis, AFIT/GIR/ENV/01M-011. School of Engineering and Management, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, February 2001.

Lenth, Russ. Statistical tool for power and sample size. http://www.stat.uiowa.edu/~rlenth/power/index.html. Undated.

Levine, Timothy R. and Steven A. McCornack. "The Dark Side of Trust: Conceptualizing and Measuring Types of Communicative Suspicion," Communication Quarterly 4: 325-340 (Fall 1991).

-----. "Linking Love and Lies: A Formal Test of the McCornack and Parks Model of Deception Detection," Journal of Social and Personal Relationships, 9: 143-154 (1992).

McCornack, Steven A. "Information Manipulation Theory," Communication Monographs, 59: 1-15 (March 1992).

McCornack, Steven A. and Timothy R. Levine. "When Lovers Become Leery: The Relationship Between Suspicion and Accuracy in Detecting Deception," Communication Monographs, 57: 219-229 (September 1990).

McCornack, Steven A. and Malcolm R. Parks. "Deception Detection and Relationship Development: The Other Side of Trust," in Communication Yearbook, 9. Ed. Margaret L. McLaughlin. Newbury Park, CA: Sage Publications, 1986.

Miller, Gerald R. and James B. Stiff. Deceptive Communication. Newbury Park, CA: Sage Publications, 1993.

Moray, Neville, Douglas Hiskes, John lee, and Bonnie M. Muir. "Trust and Human Intervention in Automated Systems," in Expertise and Technology: Cognition and Human-Computer Cooperation. Eds. Jean-Michel Hoc and Pietro Carlo Cacciabue. Hillsdale, NJ: Lawrence Erlbaum Associates, Inc., 1995.

Muir, Bonnie M. "Trust Between Humans and Machines, and the Design of Decision Aids," International Journal of Man-Machine Studies 27: 527-539 (1987).

-----. "Trust in Automation: Part I. Theoretical Issues in the Study of Trust and Human Intervention in Automated Systems," Ergonomics 37(11): 1905-1922 (1994).

Skitka, Linda J., Kathleen L. Mosier, and Mark Burdick. "Does Automation Bias Decision-making?" International Journal of Human-Computer Studies 51: 991-1006 (1999).

Toris, Carol, and Bella M. DePaulo. "Effects of Actual Deception and Suspiciousness of Deception on Interpersonal Perceptions," Journal of Personality and Social Psychology 47: 1063-1073 (1985).

Vrij, Aldert. "Credibility Judgments of Detectives: The Impact of Nonverbal Behavior, Social Skills, and Physical Characteristics on Impression Formation," Journal of Social Psychology, 133(5): 601-611 (1993).

Vrij, Aldert and Gun R. Semin. "Insight into Behavior Displayed During Deception." Human Communication Research, 22(4): 544-563 (June 1996).

Webster's II New Riverside Dictionary. New York NY: The Berkley Publishing Group, 1984.

Zmud, Robert W. "Opportunities for Strategic Information Manipulation Through New Information Technology," in Organizations and Communication Technology. Eds. Fulk and Steinfield. Sage, 1990.

Zuckerman, M., R.E. Koestner, and A. Alton. "Learning to Detect Deception," Journal of Personality and Social Psychology, 46: 519-528 (1984).

Vita

Captain Elizabeth A. Autrey was born in Pittsburgh, Pennsylvania. Her formative years were spent in Maine, where she graduated from Medomak Valley High School in 1991. Captain Autrey attended West Virginia Wesleyan College where she received a Bachelor of Science in Mathematics and a second major in Secondary Education in May of 1995. She was commissioned in June 1996 through Air Force Officer Training School.

Captain Autrey's first assignment was to the Air Force Communications Agency, Scott Air Force Base, Illinois where she initially worked in the Combat Information Transport System lead agency office. While assigned to AFCA, Captain Autrey transferred to the Scope Network division, where she worked with team members to assist Network Control Center personnel throughout the Air Force in optimizing their base computer networks. In August of 1999, she entered the Graduate School of Engineering and Management, Air Force Institute of Technology. Upon graduation, she will be assign to the 21 Communications Squadron at Peterson Air Force Base, Colorado.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to an penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
20-03-2001	Master's Thesis	Sep 1999 – Mar 2001

4. TITLE AND SUBTITLE
THE EFFECT OF CONTEXTUAL-BASED TRAINING ON ARTIFACT-BASED DECEPTION DETECTION

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Autrey, Elizabeth A., Captain, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 P Street, Building 640
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENV/01M-15

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AFOSR
ATTN: Dr. Robert L. Herklotz
Program Manager: Software and Systems
801 N. Randolph St., Room 732
Arlington, VA 22203-1977 (703) 696-6565

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Air Force dependence on information technology (IT) creates vulnerabilities that it cannot ignore. With global availability of commercial IT and the Internet, the Air Force does not necessarily have the high technological advantage over potential adversaries that it once had. Furthermore, it is possible to directly and covertly manipulate information within information systems, or artifacts, without notice. This directly affects decision makers since the availability and integrity of information is critical. Air Force physical and network security measures taken to protect its information does not guarantee detection of direct information manipulation. This leaves it to information artifact users to detect such deception. This thesis explores whether information artifact users can be trained in artifact-based deception detection. Research in this area is lacking. This study attempted to apply the contextual-based principles of Information Manipulation Theory (IMT), a theory from interpersonal deception, to human-artifact deception. An experiment comparing differences in subject performance between two Command and Control computer simulations was conducted. A training program developed from IMT principles was applied between simulations. Results of the experiment were inconclusive. Lessons learned for future research suggest training programs in human-artifact deception detection need to be both information system- and domain-specific.

15. SUBJECT TERMS

Training; Information Artifact; Deception Detection; Automation Bias

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Major David P. Biros, ENV
U	U	U	UU	102	19b. TELEPHONE NUMBER *(Include area code)* (937) 255-3636, ext 4826

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18